4600 Series IP Telephone LAN Administrator Guide

555-233-507
Issue 5
November 2006

© 2006 Avaya Inc.
All Rights Reserved.

Notice

While reasonable efforts were made to ensure that the information in this document was complete and accurate at the time of printing, Avaya Inc. can assume no liability for any errors. Changes and corrections to the information in this document may be incorporated in future releases.

For full legal page information, please see the complete document, Avaya Legal Page for Hardware Documentation, Document number 03-600759.

To locate this document on our Web site, simply go to http://www.avaya.com/support and search for the document number in the search box.

Documentation disclaimer

Avaya Inc. is not responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. Customer and/or End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation to the extent made by the Customer or End User.

Link disclaimer

Avaya Inc. is not responsible for the contents or reliability of any linked Web sites referenced elsewhere within this documentation, and Avaya does not necessarily endorse the products, services, or information described or offered within them. We cannot guarantee that these links will work all of the time and we have no control over the availability of the linked pages.

Warranty

Avaya Inc. provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available through the following Web site:

http://www.avaya.com/support

Copyright

Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights. Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

Avaya support

Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site:

http://www.avaya.com/support

Software License

USE OR INSTALLATION OF THE PRODUCT INDICATES THE END USER'S ACCEPTANCE OF THE TERMS SET FORTH HEREIN AND THE GENERAL LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE AT http://support.avaya.com/LicenseInfo/ ("GENERAL LICENSE TERMS"). IF YOU DO NOT WISH TO BE BOUND BY THESE TERMS, YOU MUST RETURN THE PRODUCT(S) TO THE POINT OF PURCHASE WITHIN TEN (10) DAYS OF DELIVERY FOR A REFUND OR CREDIT.

Avaya grants End User a license within the scope of the license types described below. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the Documentation or other materials available to End User. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users. "Software" means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone Products or pre-installed on Hardware. "Hardware" means the standard hardware Products, originally sold by Avaya and ultimately utilized by End User.

License Type(s):

Designated System(s) License (DS). End User may install and use each copy of the Software on only one Designated Processor, unless a different number of Designated Processors is indicated in the Documentation or other materials available to End User. Avaya may require the Designated Processor(s) to be identified by type, serial number, feature key, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Third-party Components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information identifying Third Party Components and the Third Party Terms that apply to them is available on Avaya's Web site at:

http://support.avaya.com/ThirdPartyLicense/

Interference

Using a cell, mobile, or GSM telephone, or a two-way radio in close proximity to an Avaya IP Telephone might cause interference.

Security

See http://support.avaya.com/security to locate and/or report known vulnerabilities in Avaya products. See http://support.avaya.com to locate the latest software patches and upgrades. For information about secure configuration of equipment and mitigation of toll fraud threats, see the Avaya Toll Fraud and Security Handbook at http://support.avaya.com.

Contents

Chapter 1: Introduction 9
About This Guide 9
Intended Audience 10
Document Organization 11
Change History 12
What's New in Issue 5 13
Terms Used in This Guide 14
Conventions Used in This Guide 17
Symbolic Conventions 17
Typographic Conventions 17
Online Documentation 17
Related Documents 18
IETF Documents 22
ITU Documents 24
ISO/IEC, ANSI/IEEE Documents 25
Customer Support 25

Chapter 2: Overview of Voice over IP (VoIP) and Network Protocols . . 27
Introduction 27
Overview of Voice over IP (VoIP) 27
Data and Voice Network Similarities 27
Delay and Jitter 28
Tandem Coding 29
Voice Coding Standards 29
Telephony Protocols 29
DHCP 29
TFTP 30
HTTP 30
DNS 30
NAT 31
QoS 31
SNMP 32
Network Assessment 32
4600 Series IP Telephones 33
Software 34
DHCP and File Servers 34
H.323 35
Registration and Authentication 35

SIP 35
Registration and Authentication 35
WAN Considerations 35
Initialization Process 36
Step 1: Telephone to Network 36
Step 2: DHCP Server to Telephone 36
Step 3: Telephone and File Server 36
Step 4: Telephone and the Call Server 37
TCP/UDP Port Utilization 38
Suggestions for Installation and Configuration 42
Reliability and Performance 42
IP Address Lists and Station Number Portability 43
Security 44

Chapter 3: Requirements 47
Introduction 47
Hardware Requirements 47
Additional Hardware Requirements 49
Software Requirements 50

Chapter 4: Server Administration 51
Introduction 51
Parameter Data Precedence 54
Administering H.323 and SIP IP Telephones on the Same Network 54
Administering 4600 Series IP Telephones on Avaya Media Servers (H.323 Only). 55
DEFINITY Releases 9, 9.5, 10, and Avaya Communication Manager Software Release 1.1+ 55
DEFINITY Release 8.4 55
DHCP and File Servers 56
Software Checklist 56
Required Network Information 56
DHCP 58
Choosing a DHCP Configuration 58
DHCP Software Alternatives 58
DHCP Generic Setup 59
Windows NT 4.0 DHCP Server 63
Verifying the Installation of the DHCP Server 63
Initial Configuration 63
Creating a DHCP Scope for the IP Telephones 64

Editing Custom Options 65
Adding the DHCP Option 66
Activating the Leases 66
Verifying Your Configuration 66
Windows 2000 DHCP Server 67
Verifying the Installation of the DHCP Server 67
Adding DHCP Options 70
Activating the New Scope 71
TFTP (H.323 Only) 71
TFTP Generic Setup 72
TFTP Server on S8300 Media Server 72
Avaya File Server Application 72
HTTP 73
HTTP Generic Setup 73
4600 Series IP Telephone Scripts and Application Files 74
Choosing the Right Application File and Upgrade Script File 76
Contents of the Upgrade Script 78
Contents of the Settings File 78
The GROUP System Value 79
QoS 80
IEEE 802.1D and 802.1Q 81
DIFFSERV 82
UDP Port Selection (H.323 Only) 83
Network Audio Quality Display on 4600 Series IP Telephones 83
RSVP and RTCP 85
Internal Audio Parameters 85
VLAN Considerations 86
VLAN Tagging 86
VLAN Detection 87
VLAN Separation 88
Unnamed Registration 89
IEEE 802.1X 90
802.1X Pass-Through and Proxy Logoff 90
802.1X Supplicant Operation 91
Link Layer Discovery Protocol (LLDP) 92
Administering Options for the 4600 Series IP Telephones 96
DNS Addressing 107
Customizing the Site-Specific Option Number (SSON) 108
Entering Options Using the Telephone Dialpad 108

Enhanced Local Dialing 108
Setting the Date and Time on SIP IP Telephones 110
Setting the Dial Plan on SIP IP Telephones 110
Customizing the 4630/4630SW IP Telephone 111
4630/4630SW Backup/Restore 114
Call Log Archive 115
Customizing 4610SW, 4620/4620SW, 4621SW, 4622SW, and 4625SW IP Telephones 116
The Application Status Flag (APPSTAT) 119
Backup/Restore for 4610SW, 4620/4620SW, 4621SW, 4622SW and 4625SW IP Telephones 121

Chapter 5: Troubleshooting Guidelines 123
Introduction 123
Error Conditions 123
The Clear Administrative Option 130
The Reset Administrative Option 132
Reset System Values 132
Restart the Telephone 134
The View Administration Option 135
Error Messages 138
Troubleshooting the 4601 IP Telephone 145

Appendix A: Avaya - 46xx IP Telephone MIB 149
Downloading the Avaya - 46xx IP Telephone MIB 149

Appendix B: Creating Web Sites for the 4630/4630SW IP Telephone 151
Introduction 151
General Background. 152
Browser Features and Behavior 152
Document Skeleton 153
Content-Based Style 153
Logical Style 154
Physical Style 155
Physical Spacing and Layout 155
Lists and Tables 156
Lists 156
Tables 156

Images 157
Links 157
Frames 158
Forms 158
Character Entities 159
Colors 160
Fonts 160
Cookies 160
Design Guidelines 161
Fixed-Width Objects 161
Images 161
Frames 162
Fonts 162
Maintaining Context 163
User Interaction 163
Click-to-Dial Functionality 164

Appendix C: Creating Web Sites for Other 4600 Series IP Telephones 167
Introduction 167

Appendix D: Administering Thin Client Directories 169
Introduction 169

Appendix E: The Push Feature 171
Introduction 171
Push Content 171
Push Priorities 172
For More Information on Push 172

Appendix F: Sample Upgrade Script File 173
Introduction 173

Index 185

Chapter 1: Introduction

About This Guide

This guide provides a description of Voice over IP and describes how to administer the DHCP, TFTP, and HTTP servers. It also covers how to troubleshoot operational problems with the 4600 Series IP Telephones and the servers.

The 4600 Series IP Telephone product line supports two signaling protocols - the Session Initiation Protocol (SIP) and the H.323 protocol. The chart below shows the 4600 Series IP Telephone models and the protocol(s) they support.

IP Telephone Model	H323 Protocol Supported?	SIP Protocol Supported?
4601	Yes	No
4601+	Yes	No
4602	Yes	Yes
4602SW	Yes	Yes
4602SW+	Yes	Yes
4606	Yes	No
4610SW	Yes	Yes
4612	Yes	No
4620	Yes	No
4620SW	Yes	Yes
4621SW	Yes	Yes
4622SW	Yes	No
4624	Yes	No
4625SW	Yes	No
4630	Yes	No
4630SW	Yes	No
4690	Yes	No

Sets that support both protocols, for example, the 4610SW, do not support each protocol simultaneously. Instead, a given telephone must be loaded with software that supports one protocol or the other.

Telephones with H.323 software work only with Avaya Communication Manager call servers. Telephones with SIP software are supported only in Avaya server environments.

Note:

Unless otherwise indicated, any reference to "the DEFINITY® server" in this document also refers to the Avaya Communication Manager media servers.

Administration of the 4602/4602SW SIP Telephones with Release 1.x software is not covered in this guide. See the *4602 SIP Telephone Administrator's Guide* (Document Number 16-300037) for information on administering these 4602/4602SW SIP Telephones.

Intended Audience

This document is intended for personnel who administer:

- DHCP, TFTP, HTTP, SIP Registration and/or other servers to support the 4600 Series SIP IP and IP Telephones, and
- Local Area Networks.

CAUTION:

Avaya does not support many of the products mentioned in this document. Take care to ensure that there is adequate technical support available for these types of servers:

- TFTP servers,
- HTTP servers,
- DHCP servers,
- SIP Registration servers,
- FTP servers,
- LDAP servers, and
- Web servers.

Note: If the servers are not functioning correctly, the 4600 Series IP Telephones may not operate correctly.

Document Organization

The guide contains the following sections:

Chapter 1: Introduction	Provides an overview of the 4600 Series IP Telephone LAN Administrator document.
Chapter 2: Overview of Voice over IP (VoIP) and Network Protocols	Describes VoIP and factors influencing its performance that must be considered when implementing this feature.
Chapter 3: Requirements	Describes the hardware and software requirements for Avaya's VoIP offering.
Chapter 4: Server Administration	Describes DHCP, TFTP, and HTTP administration for the 4600 Series IP and SIP IP Telephones.
Chapter 5: Troubleshooting Guidelines	Describes messages that might occur during the operation of the 4600 Series IP Telephones.
Appendix A: Avaya - 46xx IP Telephone MIB	Provides a link to the MIB specification for the 46xx IP Telephones: 4601, 4601+, 4602/4602SW/4602SW+, 4606, 4610SW, 4612, 4620/4620SW, 4621SW, 4622SW, 4624, 4625SW, and 4630/4630SW.
Appendix B: Creating Web Sites for the 4630/4630SW IP Telephone	Provides information on creating and customizing Web sites for viewing on the 4630/4630SW IP Telephone. Also describes the current capabilities and limitations of the 4630/4630SW's Web Browser.
Appendix C: Creating Web Sites for Other 4600 Series IP Telephones	Provides information on creating and customizing Web sites for viewing on the 4610SW, 4620/4620SW, 4621SW, 4622SW, and 4625SW IP Telephones.
Appendix D: Administering Thin Client Directories	Provides information on administering an LDAP directory for the 4610SW, 4620/4620SW, 4621SW, 4622SW, and 4625SW IP Telephones.
Appendix E: The Push Feature	Provides information about the Push feature available as of Release 2.1.
Appendix F: Sample Upgrade Script File	Provides a detailed example of a 46xx upgrade script file.

Change History

Issue 1.0	This document was issued for the first time in November 2000.
Issue 1.1	This version of the document, revised and issued in April 2001, supports through DEFINITY® Release 9.
Issue 1.5	This version of the document was revised in June, 2001 to support DEFINITY® Release 9.5.
Issue 1.6	This version of the document was revised to support DEFINITY® Release 10 and the 4630 IP Telephone.
Issue 1.7	This version of the document was revised in July, 2002 to support Avaya Communication Manager Release 1.1 and the 4602 and 4620 IP Telephones.
Issue 1.8	This version of this document was revised in June, 2003 to support Avaya Communication Manager Releases 1.2 and 1.3. This version also supported the 4602SW and 4630SW IP Telephones.
Issue 2.0	This version of this document was revised in December, 2003 to add support for Avaya Communication Manager Release 2.0. This version also supported the 4610SW and 4620SW IP Telephones, and the 4690 IP Conference Telephone.
Issue 2.1	This version of this document was revised in July, 2004 to add support for Avaya Communication Manager Release 2.1. This version also added support for the TFTP server on the Avaya S8300 Media Server, and support for the 4601 IP Telephone.
Issue 2.2	This version of this document was revised and issued in April, 2005. This version supports through Avaya Communication Manager Release 2.2. This version also introduces the 4621SW, 4622SW, and 4625SW IP Telephones.
Issue 2.2.1	This version of this document was revised and issued in August, 2005. This version introduced the SIP IP Telephones. This version also distinguishes between functionality that is H.323-specific and functionality that is SIP-specific.
Issue 2.3	This version of this document was revised and issued in November, 2005 to provide support through Avaya Communication Manager Release 3.0.
Issue 3	This version of this document was revised and issued in April, 2006 to support Software Release 2.4. This version provides VLAN separation parameters, an unnamed registration parameter, and audio customization parameters.
Issue 4	This version of this document was revised and issued in August, 2006. This version supports Avaya Communication Manager 3.1 and Software Release 2.6. New features for 802.1X authentication, Link Layer Discovery Protocol (LLDP), and power conservation are introduced.
Issue 5	This is the current version of this document, revised and issued in November, 2006 to support Software Release 2.7. This version introduces additional Unicode languages, support for dialpad-activated Web links, the capability to turn off the display backlight, several new system parameters, and two new local procedures. This issue also introduces new telephone models 4601+ and 4602SW+, which replace the 4601 and 4602/4602SW, respectively. What's New in Issue 5 describes Release 2.7 in more detail.

What's New in Issue 5

New material in this issue to support Release 2.7 software includes:

- 4625SW IP Telephones now support all the applications and functionality that 4620SW IP Telephones have supported since Software Release 2.1. Differences are that the 4625 has a color 1/4-VGA display, has a slightly different stand, and does not have an infrared (IR) interface.
- Support for the following Unicode languages on the 4625SW IP Telephone:
  - Simplified Chinese,
  - Korean,
  - Russian, and
  - Hebrew.
- User selection of color schemes on 4625SW IP Telephones.
- New system parameters BAKLIGHTOFF, FTPDIR, FTPSRVR, FTPUSERSTAT, HEADSYS, QKLOGINSTAT, UNNAMEDSTAT, WMLIDLETIME, and WMLIDLEURI. See Table 10 for information.
- Two local administrative procedures, described in detail in the *4600 Series IP Telephone Installation Guide* (Document Number 555-233-128):
  - Mute C O N T # - to allow users to adjust telephone display contrast, and
  - Mute O F F # - to immediately turn off the display backlight.
- Support for the 4601+ and 4602SW+ IP Telephones, which replace the 4601, 4602, and 4602SW IP Telephones, respectively. Release 2.7 does not support the 4601, 4602, and 4602SW IP Telephones.
- The 4610SW, 4620SW, 4621SW, 4622SW IP Telephones now support the Korean language.
- Appendix F: Sample Upgrade Script File was added to replace an older sample previously in Chapter 4.

Terms Used in This Guide

802.1D **802.1Q**	802.1Q defines a layer 2 frame structure that supports VLAN identification and a QoS mechanism usually referred to as 802.1D.
802.1X	Authentication method for a protocol requiring a network device to authenticate with a back-end Authentication Server before gaining network access. Applicable 4600 Series IP telephones support IEEE 802.1X as a Supplicant with the EAP-MD5 authentication method.
ARP	Address Resolution Protocol, used, for example, to verify that the IP Address provided by the DHCP server is not in use by another IP telephone.
CELP	Code-excited linear-predictive. Voice compression requiring only 16 kbps of bandwidth.
CLAN	Control LAN, type of Gatekeeper circuit pack.
CNA	Converged Network Analyzer, an Avaya product to test and analyze network performance.
DHCP	Dynamic Host Configuration Protocol, an IETF protocol used to automate IP Address allocation and management.
DiffServ	Differentiated Services, an IP-based QoS mechanism.
DNS	Domain Name System, an IETF standard for ASCII strings to represent IP Addresses.
EAP	Extensible Application Protocol.
Gatekeeper	H.323 application that performs essential control, administrative, and managerial functions in the media server. Sometimes called CLAN in Avaya documents.
H.323	A TCP/IP-based protocol for VoIP signaling.
HTTP	Hypertext Transfer Protocol, used to request and transmit pages on the World Wide Web.
HTTPS	A secure version of HTTP.
IETF	Internet Engineering Task Force, the organization that produces standards for communications on the internet.
LAN	Local Area Network.
LDAP	Lightweight Directory Access Protocol, an IETF standard for database organization and query exchange.

1 of 3

LLDP	Link Layer Discovery Protocol. All IP telephones with an Ethernet interface support the transmission and reception of LLDP frames on the Ethernet line interface in accordance with IEEE standard 802.1AB.
MAC	Media Access Control, ID of an endpoint.
Media Channel Encryption	Encryption of the audio information exchanged between the IP telephone and the call server or far end telephone.
NAPT	Network Address Port Translation.
NAT	Network Address Translation.
OPS	Off-PBX Station.
PAE	Port Access Entity. The protocol entity associated with a port. The PAE supports the protocol functionality associated with the authenticator, supplicant, or both.
PHP	Hypertext Preprocessor, software used to assist in the format and display of Web pages.
PoE	Power over Ethernet.
PSTN	Public Switched Telephone Network, the network used for traditional telephony.
QoS	Quality of Service, used to refer to several mechanisms intended to improve audio quality over packet-based networks.
Registration Server	A SIP server that accepts REGISTER requests. The Registration Server places the information received in the requests into the location service for the domain the server handles.
RSVP	Resource ReSerVation Protocol, used by hosts to request resource reservations throughout a network.
RTCP	RTP Control Protocol, monitors quality of the RTP services and can provide real-time information to users of an RTP service.
RTP	Real-time Transport Protocol. Provides end-to-end services for real-time data such as voice over IP.
SDP	Session Description Protocol. A well-defined format for conveying sufficient information to discover and participate in a multimedia session.
Signaling Channel Encryption	Encryption of the signaling protocol exchanged between the IP telephone and the call server. Signaling channel encryption provides additional security to the security provided by media channel encryption.

2 of 3

SIP	Session Initiation Protocol. An IETF standard protocol for IP communication. SIP enables IP telephony gateways, client endpoints, PBXs, and other communication systems or devices to communicate with each other. SIP mainly addresses the call setup and tear down mechanisms of sessions and is independent of the transmission of media streams between the caller and the party called. SIP is an alternative to H.323 for VoIP signaling.
SNMP	Simple Network Management Protocol. The Internet standard protocol, defined in STD 15, RFC 1157, developed to manage nodes on an IP network.
SNTP	Simple Network Time Protocol. An adaptation of the Network Time Protocol used to synchronize computer clocks in the internet.
Supplicant	An entity at one end of a point-to-point LAN segment that is being authenticated by an authenticator at the other end.
TCP/IP	Transmission Control Protocol/Internet Protocol, a network-layer protocol used on LANs and internets.
TFTP	Trivial File Transfer Protocol, used to provide downloading of upgrade scripts and application files to the IP telephones.
TLS	Transport Layer Security, an enhancement of Secure Sockets Layer (SSL). TLS is compatible with SSL 3.0 and allows for privacy and data integrity between two communicating applications.
TLV	Type-Length-Value elements transmitted and received as part of Link Layer Discovery Protocol (LLDP).
UDP	User Datagram Protocol, a connectionless transport-layer protocol.
Unnamed Registration	Registration with Avaya Communication Manager by an IP telephone with no extension. Unnamed registration is typically used to limit outgoing calling.
VLAN	Virtual LAN.
VoIP	Voice over IP, a class of technology for sending audio data and signaling over LANs.
WML	Wireless Markup Language, used by the 4620 Web Browser to communicate with WML servers.

3 of 3

Conventions Used in This Guide

This guide uses the following textual, symbolic, and typographic conventions to help you interpret information.

Symbolic Conventions

Note:

This symbol precedes additional information about a topic. This information is not required to run your system.

CAUTION:

This symbol emphasizes possible harm to software, possible loss of data, or possible service interruptions.

Typographic Conventions

This guide uses the following typographic conventions:

`command`	Words printed in this type are commands that you enter into your system.
`message`	Words printed in this type are system messages.
device	Words printed in this type indicate parameters associated with a command for which you must substitute the appropriate value. For example, when entering the **`mount`** command, ***device*** must be replaced with the name of the drive that contains the installation disk.
Administrative	Words printed in bold type are menu or screen titles and labels. Words printed in bold type can also be items on menus and screens that you select or enter to perform a task, i.e., fields, buttons, or icons. Bold type also provides general emphasis for words or concepts.
italics	Italic type indicates a document that contains additional information about a topic.

Online Documentation

The online documentation for the 4600 Series IP Telephones is located at the following URL:

http://www.avaya.com/support

Related Documents

- *DEFINITY® ECS (Enterprise Communication Server) Documentation Release 8.4*

  This CD contains documentation that describes, among other things, how to administer a DEFINITY ECS switch with Release 8.4 software. This document is provided with the DEFINITY Release 8.4 product.

- *DEFINITY® ECS (Enterprise Communication Server) Documentation Release 9*

  This CD contains documentation that describes, among other things, how to administer a DEFINITY ECS switch with Release 9 software. This document is provided with the DEFINITY Release 9 product.

- *DEFINITY® ECS (Enterprise Communication Server) Documentation Release 10*

  This CD contains documentation that describes, among other things, how to administer a DEFINITY ECS switch with Release 10 software. This document is provided with the DEFINITY Release 10 product.

- *Avaya Communication Manager Software Documentation Release 1.1*

  This document describes how to administer a switch with Avaya Communication Manager software. This document is provided with the Avaya Communication Manager Release 1.1 product.

- *Avaya Communication Manager Software Documentation Release 1.2*

  This document describes how to administer a switch with Avaya Communication Manager software. This document is provided with the Avaya Communication Manager Release 1.2 product.

- *Avaya Communication Manager Documentation Release 1.3*

  This document describes how to administer a switch with Avaya Communication Manager software. This document is provided with the Avaya Communication Manager Release 1.3 product.

- *Avaya Communication Manager Documentation Release 2.0*

  This document describes how to administer a switch with Avaya Communication Manager software. This document is provided with the Avaya Communication Manager Release 2.0 product.

- *Avaya Communication Manager Documentation Release 2.1*

  This document describes how to administer a switch with Avaya Communication Manager software. This document is provided with the Avaya Communication Manager Release 2.1 product.

- *Avaya Communication Manager Documentation Release 2.2*

  This document describes how to administer a switch with Avaya Communication Manager software. This document is provided with the Avaya Communication Manager Release 2.2 product.

- *Avaya Communication Manager Documentation Release 3.0*

  This document describes how to administer a switch with Avaya Communication Manager software. This document is provided with the Avaya Communication Manager Release 3.0 product.

- *Avaya Communication Manager Documentation Release 3.1*

  This document describes how to administer a switch with Avaya Communication Manager software. This document is provided with the Avaya Communication Manager Release 3.1 product.

The following documents are available on the Web site listed under Online Documentation:

- *Avaya IP Telephone SNMP Security White Paper*, Issue 0.1

  This document has extensive information about SNMP and related Release 2.6 changes.

- *Administration for Network Connectivity for Avaya Communication Manager Software* (555-233-504)

  This document describes how to administer Avaya Communication Manager software to implement Voice over IP (VoIP) applications for TCP/IP for DCS signaling, H.323 trunks, and private networks.

- *Administrator Guide for Avaya Communication Manager* (03-300509)

  This document provides an overall reference for planning, operating, and administering your Avaya Communication Manager solution.

- *Installation and Upgrades for Avaya G700 Media Gateway and Avaya S8300 Media Server* (555-234-100)

  This document describes procedures for installing, upgrading, and performing initial configuration tasks for the Avaya G700 Media Gateway and the Avaya S8300 Media Server.

- *Downloading Avaya 46xx IP Telephone Software Using Avaya Media Servers*

  This White Paper provides information on using HTTP/HTTPS or TFTP file transfer protocols to transfer Avaya 46xx IP telephone software from Avaya Media Servers to Avaya 46xx IP telephones.

- *SIP Support in Release 3.0 of Avaya Communication Manager running on the Avaya S8300, S8500, and 8710 Media Server* (555-245-206)

  This document describes requirements and introduces procedures for administering SIP (Session Initiation Protocol) with Avaya Communication Manager Release 3.0.

- *Converged Communications Server Release 3.0 Installation and Administration* (555-245-705)

  This document describes procedures for installing and administering the Converged Communication Server, used by Session Initiation Protocol (SIP) IP Telephones.

- *Avaya Extension to Cellular and Off-PBX Station (OPS) Installation and Administration Guide* (210-100-500)

  This document describes the installation, administration, maintenance, and troubleshooting tasks necessary to install and set up Avaya Extension to Cellular and Off-PBX Stations.

- *Avaya IP Telephone File Server Application Reference Guide* (16-601433)

  This document describes how to install and implement the File Server Application for IP Telephones.

- *4600 Series IP Telephones Safety Instructions* (555-233-779)

  This document contains important user safety instructions for the 4600 Series IP Telephones.

- *30A Switched Hub Set Up Quick Reference, Issue 2, July 2002* (555-236-700)

  This document contains important safety and installation information for the 30A Switched Hub.

- *4600 Series IP Telephone Installation Guide* (555-233-128)

  This document describes how to install 4600 Series IP Telephones. It also provides troubleshooting guidelines for the 4600 Series IP Telephones.

- *4600 Series IP Telephones Application Programmer Interface (API) Guide* (16-300256)

  This document provides information on developing Web applications for 4610SW, 4620/4620SW, 4621SW, 4622SW, and 4625SW IP Telephones. This document also covers Push feature administration.

- *4601 IP Telephone User Guide* (16-300043)

  This document provides detailed information about using the 4601 and 4601+ IP Telephone.

- *4602/4602SW IP Telephone User Guide* (555-233-780)

  This document provides detailed information about using the 4602/4602SW/4602SW+ IP Telephone.

- *4602/4602SW SIP IP Telephone User Guide* (16-300470)

  This document provides detailed information about using the 4602/4602SW SIP IP Telephone.

- *4606 IP Telephone User Guide* (555-233-775)

  This document provides detailed information about using the 4606 IP Telephone.

- *4610SW IP Telephone User Guide* (555-233-784)

  This document provides detailed information about using the 4610SW IP Telephone.

- *4610SW SIP IP Telephone User Guide* (16-300472))

  This document provides detailed information about using the 4610SW SIP IP Telephone.

- *4612 IP Telephone User Guide (*555-233-777)

  This document provides detailed information about using the 4612 IP Telephone.

- *4620/4620SW/4621SW IP Telephone User Guide* (555-233-781)

  This document provides detailed information about using the 4620/4620SW and 4621SW IP Telephones.

- *4620SW/4621SW SIP IP Telephone User Guide* (16-300474)

  This document provides detailed information about using the 4620SW and 4621SW SIP IP Telephones.

- *4622SW IP Telephone User Guide* (16-300297)

  This document provides detailed information about using the 4622SW IP Telephone.

- *4624 IP Telephone User Guide* (555-233-776)

  This document provides detailed information about using the 4624 IP Telephone.

- *4625SW IP Telephone User Guide* (16-300298)

  This document provides detailed information about using the 4625SW IP Telephone.

- *4630/4630SW IP Telephone User Guide* (555-233-764)

  This document provides detailed information about using the 4630/4630SW IP Telephone.

- *Avaya 4690 IP Conference Telephone User Guide* (555-233-787)

  This document provides detailed information about using the 4690 IP Conference Telephone.

- *4601/4602/4602SW IP Telephone Stand Instructions* (555-233-147)

  This document provides information on how to desk- or wall-mount a 4601 or 4602/4602SW IP Telephone and a 4602/4602SW SIP IP Telephone.

- *4610SW IP Telephone Stand Instructions* (555-233-165)

  This document provides information on how to desk- or wall-mount a 4610SW IP or SIP IP Telephone.

- *4620/4620SW/4621SW/4622SW/4625SW IP Telephone Stand Instructions* (16-300299)

  This document provides information on how to mount a 4620/4620SW/4621SW/4622SW/4625SW IP or 4620SW/4621SW SIP IP Telephone on a wall.

IETF Documents

The following documents provide standards relevant to IP Telephony and are available for free from the IETF Web site: http://www.ietf.org/rfc.html.

- *Requirements for Internet Hosts - Communication Layers*, October 1989, by R. Braden (STD 3: RFC 1122)
- *Requirements for Internet Hosts - Application and Support*, October 1989, by R. Braden (STD 3: RFC 1123)
- *Internet Protocol (IP)*, September 1981, by Information Sciences Institute (STD 5: RFC 791), as amended by *Internet Standard Subnetting Procedure*, August 1985, by J. Mogul and J. Postel (STD 5: RFC 950)
- *Broadcasting Internet Datagrams*, October 1984, by J. Mogul (STD 5: RFC 919)
- *Broadcasting Internet Datagrams in the Presence of Subnets*, October 1984, by J. Mogul (STD 5: RFC 922)
- *User Datagram Protocol (UDP)*, August 28, 1980, by J. Postel (STD 6: RFC 768)
- *Transmission Control Protocol (TCP)*, September 1981, by Information Sciences Institute (STD 7: RFC 793)
- Domain Names - Concepts and Facilities (DNS), November, 1987, by P. Mockapetris (STD 13: RFC 1034)
- Domain Names - Implementation and Specification (DNS), November 1987, by P. Mockapetris (STD 13: RFC 1035)
- *The TFTP Protocol (Revision 2), (TFTP)*, July 1992, by K. Sollins, (STD 33: RFC 1350:) as updated by *TFTP Option Extension*, May 1998, by G. Malkin and A. Harkin (RFC 2347)
- *An Ethernet Address Resolution Protocol (ARP)*, November 1982, by David C. Plummer (STD 37: RFC 826)
- *Dynamic Host Configuration Protocol (DHCP)*, March 1997, by R. Droms (RFC 2131)
- *DHCP Options and BOOTP Vendor Extensions*, March 1997, by S. Alexander and R. Droms (RFC 2132)
- *RTP: A Transport Protocol for Real-Time Applications (RTP/RTCP)*, January 1996, by H. Schulzrinne, S. Casner, R. Frederick, V. Jacobson (RFC 1889)
- *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*, *(DIFFSRV)*, December 1998, by K. Nichols, S. Blake, F. Baker and D. Black (RFC 2474)
- *Introduction to version 2 of the Internet-standard Network Management Framework (SNMPv2),* April 1993, by J. Case, K. McCloghrie, M. Rose, and S. Waldbusser (RFC 1441)
- *Management Information Base for Network Management of TCP/IP Internets: MIB-II,* March 1991, edited by K. McCloghrie and M. Rose (RFC 1213)

- *SNMPv2 Management Information Base for the Internet Protocol using SMIv2,* November 1996, edited by K. McCloghrie (RFC 2011)
- *Structure of Management Information Version 2 (SMIv2),* April 1999, edited by K. McCloghrie, D. Perkins, and J. Schoenwaelder (RFC 2578)
- *Resource ReSerVation Protocol VI*, September 1997, by R. Braden, L. Zhang, S. Berson, S. Herzog, and S. Jamin (RFC 2205)
- *Lightweight Directory Access Protocol,* March 1995, by M. Wahl, T. Howes, and S. Kille (RFC 1777)
- *Lightweight Directory Access Protocol (v3),* December 1997, by M. Wahl, T. Howes, and S. Kille (RFC 2251)
- *Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions,* December 1997, by M. Wahl, Coulbeck, T. Howes, and S. Kitte (RFC 2252)
- *Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names,* December 1997, by M. Wahl, S. Kille, and T. Howes (RFC 2253)
- *The TLS Protocol Version 1.0,* January 1999, by T. Dierks and C. Allen (RFC 2246)
- *SDP: Session Description Protocol,* April 1998, by M. Handley and V. Jacobsen (RFC 2327)
- *RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals,* May 2000, by H. Schulzrinne and S. Petrack (RFC 2833)
- *SIP: Session Initiation Protocol,* June 2002, by J. Rosenberg et. al. (RFC 3261)
- *Session Initiation Protocol (SIP): Locating SIP Servers*, June 2002, by J. Rosenberg and H. Schulzrinne (RFC 3263)
- *Session Initiation Protocol (SIP) - Specific Event Notification,* June 2002, by A.B. Roach (RFC 3265)
- *The Session Initiation Protocol (SIP) Refer Method,* April 2003, by R. Sparks (RFC 3515)
- *A Message Summary and Message Waiting Indication Event Package for the Session Initiation Protocol (SIP),* August 2004, by R. Mahy (RFC 3842)

ITU Documents

The following documents are available for a fee from the ITU Web site: http://www.itu.int.

- *Recommendation G.711, Pulse Code Modulation (PCM) of Voice Frequencies*, November 1988
- *Recommendations G.726: 40, 32, 24, 16 kbit/s Adaptive Differential Pulse Code Modulation (ADPCM),* December 1990
- *G.726 Appendix II, Digital test sequences for the verification of the G.726 40, 32, 24 and 16 kbit/s ADPCM*, March 1991
- *G.726 Appendix III, comparison of ADPCM algorithms*, May 1994
- *G.726 Annex A, Extensions of Recommendation G.726 for use with uniform-quantized input and output*, November 1994
- *G.726 Annex B, Packet format capability identifier and capability parameters for H.245 signaling*, July 2003
- *Recommendation G.729, Coding of speech at 8 kbit/s using Conjugate-Structure Algebraic-Code-Excited Linear-Prediction (CS-ACELP)*, March 1996
- *Annex A to Recommendation G.729: Reduced complexity 8 kbit/s CS-ACELP speech codec*, November 1996
- *Annex B to Recommendation G.729: A silence compression scheme for G.729 optimized for terminals conforming to Recommendation V.70*, November 1996
- *Recommendation H.225.0, Call signalling protocols and media stream packetization for packet-based multimedia communications systems*, February 1998
- *Recommendation H.245, Control protocol for multimedia communication*, February 1998
- *Recommendation H.323, Packet-based multimedia communications systems*, February 1998

ISO/IEC, ANSI/IEEE Documents

The following documents are available free from the ISO/IEC standards Web site: http://www.standards.ieee.org/getieee802/portfolio.html**.**

- *International Standard ISO/IEC 8802-2:1998 ANSI/IEEE Std 802.2, 1998 Edition, Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks- Specific requirements- Part 2: Logical Link Control*
- *ISO/IEC 15802-3: 1998 ANSI/IEEE Std 802.1D, 1998 Edition, Information technology- Telecommunications and information exchange between systems- Local and metropolitan area networks- Common specifications- Part 3: Media Access Control (MAC) Bridges*
- *IEEE Std 802.1Q-1998, IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks*
- *IEEE Std 802.3af-2003, IEEE Standard for Information technology - Telecommunications and information exchange between systems- Local and metropolitan area networks- Specific requirements- Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications- Amendment: Data Terminal Equipment (DTE) Power via Media Dependent Interface (MDI)*
- *IEEE Std. 802.1X-2004, IEEE Standard for Local and Metropolitan Area Networks - Port-Based Network Access Control*
- *IEEE Std. 802.1AB-2005, IEEE Standard for Local and Metropolitan Area Networks: Station and Media Access Control Connectivity Discovery*
- For more information about 802.1AB, see: http://www.standards.ieee.org/getieee802/download/802.1AB-2005.pdf.
- For more information about 802.1X, see: http://www.standards.ieee.org/getieee802/download/802.1X-2004.pdf.

Customer Support

Call the Avaya support number provided to you by your Avaya representative or Avaya reseller for 4600 Series IP Telephone support.

Information about Avaya products can be obtained at the following URL:

http://www.avaya.com/support

Chapter 2: Overview of Voice over IP (VoIP) and Network Protocols

Introduction

This chapter describes the differences between data and voice networks, and the factors that influence the performance of VoIP. The installation and administration of 4600 Series IP Telephones on Avaya Media Servers, and the installation and configuration of DHCP and TFTP are addressed.

Overview of Voice over IP (VoIP)

The 4600 Series IP Telephones allow enterprises to use Voice over IP (VoIP). VoIP uses packet-switched networks over the Public Switched Telephone Network (PSTN) instead of telephony. However, using data networks to transmit voice packets poses a problem. Data networks were not designed for the specific qualities required by voice traffic.

Data and Voice Network Similarities

Data and voice networks share similar functions because of the nature of networking.

- **Signaling:** establishes a connection between two endpoints.

  In a voice network, signaling helps identify who the calling party is trying to call and where the called party is on the network. Traditional telephony uses terminals with fixed addresses. Traditional telephony establishes a fixed connection for the communication session between two such terminals, allocating fixed bandwidth resources for the duration of the call.

  IP communications constitute a connectionless network, having neither fixed addresses nor fixed connections.

- **Addressing:** a unique address that must identify each terminal on a network.

  In a voice network, the unique address is a permanent attribute, based on any combination of:

  - international numbering plans,
  - national numbering plans,
  - local telephone company practices,
  - internal customer-specific codes.

  In IP communications, dial plans track extension numbers assigned to terminals. No fixed connection path is needed.

- **Routing:** related to addressing and allows connections to be established between endpoints.

Although these functions are common to data and voice networks, the implementations differ.

Delay and Jitter

Data traffic is usually short and comes in bursts. Data networks like the Internet are designed to manage these bursts of traffic from many sources on a first-come, first-served basis. Data packets are sent to multiple destinations, often without any attempt to keep them in a particular order.

Voice networks are designed for continuous transmission during a call. The traffic is not bursty, and the conversation uses a specific amount of bandwidth between the two ends during the call.

Several features of data networks are unsuitable for voice telephony:

- Data network design delivers data at the destination, but not necessarily within a certain time, producing delay (latency). In data networks, delay tends to be variable. For voice messages, variable delay results in jitter, an audible choppiness in conversations.
- Variable routing also can result in loss of timing synchronization, so packets are not received at the destination in the proper order.
- Data networks have a strong emphasis on error correction, resulting in repeated transmissions.

Data network concepts include prioritization of traffic types to provide some form of greater traffic reliability, for example, for interactive transactions. However, data requirements tend to not be as strict as most voice requirements.

The 4600 Series IP Telephones include a dynamic jitter buffer. This feature automatically smooths jitter to improve audio quality.

Tandem Coding

Tandem coding, also called transcoding, refers to converting a voice signal from analog to digital and back again. When calls are routed over multiple IP facilities, they can be subject to multiple transcodings. The multiple conversions between analog and digital coding result in a deterioration in the voice quality. Avoid tandem coding wherever possible in any compressed voice system, for example, by minimizing analog trunking on the PBX.

Voice Coding Standards

There are several voice coding standards. Avaya 4600 Series IP Telephones offer these options:

- G.711, which describes the 64 kbps PCM voice coding technique. G.711-encoded voice is already in the correct format for digital voice delivery in the public telephone network or through PBXs.
- G.726 ADPCM at 32Kbps.
- G.729A and G.729B, both of which describe adaptive code-excited, linear-predictive (CELP) compression that allows voice to be coded into 8 kbps streams.

Telephony Protocols

There are two major protocols used for Voice over IP (VoIP) signaling - Session Initiation Protocol (SIP) and H.323. The two protocols provide connection control and call progress signaling, but in very different ways. These protocols can be used simultaneously over the same network, but in general, no endpoint supports both protocols at the same time. Neither protocol is necessarily superior, but each offers some unique advantages. SIP telephones, for example, do not require centralized call servers, and can route telephone calls when a URL identifies the destination. H.323 telephones leverage the call server's presence into the potential availability of hundreds of telephone-related features that a standalone SIP telephone cannot provide.

DHCP

Dynamic Host Configuration Protocol (DHCP) allows a server to assign IP Addresses and other parameters to devices like the 4600 Series IP Telephones on an as-needed basis. DHCP eliminates the need to configure each end station with a static IP Address. The DHCP application also passes information to the 4600 Series IP Telephone. The DHCP application identifies the PBX and the file server's IP Addresses. The application also identifies the paths to the upgrade script and the application file on the file server.

For further information, see DHCP and File Servers on page 56 and DHCP on page 58.

TFTP

The Avaya 4600 IP Telephones can get useful application information from the TFTP server. The telephones also can upgrade themselves using files stored on the TFTP server. After downloading software, the Avaya 4600 Series IP Telephones can operate without a file server. However, some functionality can be lost if the file server is not available for a telephone reset. For further information, see:

- DHCP and File Servers on page 56,
- TFTP (H.323 Only) on page 71, and
- Table 1: File Servers and Compatible Telephone Software.

HTTP

HTTP is potentially a more secure alternative to TFTP, particularly when Transport Layer Security (TLS) is used to create HTTPS (Secure HTTP). You can store the same application software, script file, and settings file on an HTTP server as you can on the TFTP server. With proper administration, the telephone seeks out and uses that material appropriately. However, not all 4600 Series IP Telephones support HTTP, as indicated in Table 1.

Table 1: File Servers and Compatible Telephone Software

File Server	IP Telephone Models	IP Telephone Software Release Number
HTTP, HTTPS, or TFTP	4601+, 4602SW+, 4625SW	R2.7
	4601, 4602, 4602SW, 4610SW, 4620, 4620SW, 4621SW, 4622SW	R2.2+
TFTP	4606, 4612, 4624, 4625SW, 4630, 4630SW, 4690	All releases

As with TFTP, some functionality might be lost by a reset if the HTTP server is not available. For more information, see DHCP and File Servers on page 56 and HTTP on page 73.

DNS

The Domain Name System (DNS) is a distributed Internet directory service. DNS is used mostly to translate between domain names and IP Addresses. Release 1.5 and later Avaya IP Telephones can use DNS to resolve names into IP Addresses. In DHCP, TFTP, and HTTP files, DNS names can be used wherever IP Addresses were available as long as a valid DNS server is identified first. See DNS Addressing on page 107.

NAT

A Network Address Translation (NAT) is an application that can be administered between your network and the Internet. The NAT translates network layer IP Addresses so your local intranet IP Addresses can duplicate global, Internet addresses. A detailed discussion of NAT is beyond the scope of this document. Note that NAT use can lead to problems that affect the consistency of addressing throughout your network. In Release 1.6 and earlier releases of the 4600 Series IP Telephones, NAT is **not** recommended for networks handling IP-based telephony traffic. As of Release 1.7, all 4600 Series H.323 IP Telephones support NAT interworking. Therefore, no problems exist with NAT and these H.323 IP telephones. Note that support for NAT does not imply support for Network Address Port Translation (NAPT). Specifically, the H.323 IP telephones do not support communication to the PBX through any NAPT device. SIP IP telephones do not support NAT.

NAT requires specific administration on the media server. The capability to have a direct Avaya IP Telephone-to-Avaya IP Telephone call with NAT, also called “NAT shuffling,” requires Avaya Communication Manager Release 1.3 software. See the *Administration for Network Connectivity* document listed in Related Documents on page 18.

QoS

Quality of Service (QoS) is a term covering several initiatives to maximize the voice quality heard at both ends of a call that originates or terminates on an IP-based telephone. These initiatives include various prioritization schemes to offer voice packets a larger or prioritized share of network resources. These schemes include standards such as:

- IEEE’s 802.1D and 802.1Q,
- the Internet Engineering Task Force’s (IETF’s) “Differentiated Services,”
- RTP Control Protocol (RTCP),
- Resource ReSerVation Protocol (RSVP), and
- port-based priority schemes such as UDP port selection.

Documentation for your LAN equipment details the extent to which your network can support any or all of these initiatives. See Server Administration on page 51, for some implications of QoS for the 4600 Series IP Telephones.

As of Release 1.7, the 4620, 4630, and 4630SW IP Telephones provided network audio quality information to the end user. This network audio quality information might be useful to the LAN Administrator. As of Release 1.8, all 4600 Series IP Telephones provide some level of detail about network audio quality. For specific information, see Network Audio Quality Display on 4600 Series IP Telephones on page 83.

SNMP

Simple Network Management Protocol (SNMP) is a family of standards-based protocols and procedures to allow vendor-independent data network management. Using a simple set of protocol commands, an SNMP-compliant device stores information in standard format in one or more Management Information Bases (MIBs). Usually, devices support the standards-specific MIB termed MIB-II. In addition, devices can define one or more “custom MIBs” that contain information about the device’s specifics.

As of Release 1.1, the 4600 Series IP Telephones are fully compatible with SNMPv2c, a later version of SNMP, and with Structure of Management Information Version 2 (SMIv2). The telephones respond correctly to queries from entities that comply with earlier versions of SNMP, such as SNMPv1. “Fully compatible” means that the telephones respond to queries directed either at the MIB-II or the Custom MIB. The 4600 Series IP Telephone Custom MIB is read-only. Read-only means that the values therein cannot be changed externally by means of network management tools.

You can restrict which IP Addresses the telephone accepts SNMP queries from. You can also customize your community string with system values SNMPADD and SNMPSTRING, respectively, as indicated in Chapter 4: Server Administration, Table 10: 4600 Series IP Telephone Customizable System Parameters.

Important:

SNMP has been enabled by default since Release 1.1. However, as of Release 2.6, the SNMP default changed to Null (Off). To activate SNMP, you must set SNMPSTRING to a non-null value by means of either the 46xxsettings file or DHCP Option 176 (SSON). If you use static programming, you cannot enable SNMP as of Release 2.6.

To find more information about SNMP and MIBs, see the IETF references listed in Related Documents on page 18. The Avaya Custom MIB for the 4600 Series IP Telephones is available for download in *.txt format on the Avaya support Web site. This Custom MIB is common to both H.323 and SIP IP telephones. Objects that are not relevant to a given telephone have Null data.

Network Assessment

The current technology allows optimum network configurations to deliver VoIP with perceived voice quality close to that of the Public Switched Telephone Network (PSTN). Not all networks can take advantage of packet voice transmissions. Some data networks have insufficient residual capacity for even compressed voice traffic. In addition, the usual approach to developing data networks by integrating products from many vendors requires testing the components for Voice over IP traffic compatibility.

Avaya assumes that your organization has performed a network assessment with or without Avaya's assistance before attempting to install Voice over IP. The network assessment provides a high degree of confidence that the existing data network has the capacity to carry voice packet traffic. The network assessment assures that the existing data network is compatible with the required technology.

A network assessment should include:

- A network audit to review existing equipment and evaluate its capabilities, including its ability to meet planned voice and data needs.
- A determination of network objectives, including the dominant traffic type, selection of technologies, and setting voice quality objectives.

The assessment should leave you confident that the implemented network will have the capacity for the foreseen data and voice traffic, and can support H.323, SIP, DHCP, TFTP, HTTP, and jitter buffers in all applications.

It is important to distinguish between compliance with the minimal VoIP standards and QoS support, the latter being a requirement to run VoIP on your configuration.

4600 Series IP Telephones

The 4600 Series IP Telephones support either of two signaling protocol families - H.323 and Session Initiation Protocol (SIP).

The H.323 standard, developed by ITU-T, provides for real time audio, video, and data communications transmission over a packet network. An H.323 telephone protocol stack comprises several protocols:

- H.225 for registration, admission, status (RAS), and call signaling,
- H.245 for control signaling,
- Real Time Transfer Protocol (RTP), and
- Real Time Control Protocol (RTCP).

SIP was developed by the IETF. Like H.323, SIP provides for real time audio, video, and data communications transmission over a packet network. SIP uses various messages, or methods, to provide:

- Registration (REGISTER),
- Call signaling (INVITE, BYE)
- Control signaling (SUBSCRIBE, NOTIFY)

SIP also supports RTP and RCTP using the Session Description Protocol.

A telephone is loaded with either H.323 or SIP software as part of its initial script file administration and initialization.

Software

As shipped from the factory, the 4600 Series IP Telephones may not contain the latest software. When the telephone is first plugged in, a software download from a TFTP or HTTP server starts to give the telephone its proper functionality.

For downloads of H.323 software upgrades, the PBX provides the capability for a remote restart of the 4600 Series IP Telephone. As a consequence of restarting, the telephone automatically restarts reboot procedures. If new software is available on the server, the telephone downloads it as part of the reboot process.

A 4602, 4602SW, 4602SW+, 4610SW, 4620SW, 4621SW, or 4625SW IP Telephone can support either H.323 or SIP software, but not both at the same time. All telephones come from the factory with H.323 software by default. You can convert a telephone from H.323 to SIP, or from SIP to H.323 by administering your server and settings file. For more information, see "Converting Software on Avaya 4600 Series IP Telephones" in the *4600 Series IP Telephone Installation Guide* (Document Number 555-233-128).

DHCP and File Servers

The DHCP server provides the following information to the 4600 Series IP Telephone:

- IP Address of the 4600 Series IP Telephone
- IP Address of the Gatekeeper board on the Avaya Media Server, applicable only to H.323 IP telephones
- IP Address of the TFTP server if applicable, otherwise the HTTP server
- The subnet mask
- IP Address of the router
- DNS Server IP Address

Administer the LAN so each IP telephone can access a DHCP server containing the IP Addresses and subnet mask listed.

The IP telephone cannot function without an IP Address. The failure of a DHCP server at boot time leaves all the affected voice terminals unusable. A user can manually assign an IP Address to an IP telephone. This can cause a problem when the DHCP server finally returns because the telephone never looks for a DHCP server unless the static IP data is unassigned manually. In addition, manual entry of IP data is an error-prone process. Avaya therefore **strongly recommends** that a DHCP server be available when the IP telephone reboots. If a DHCP server is not available at remote sites during WAN failures, the IP telephone is not available after a reboot.

A minimum of two DHCP servers are recommended for reliability. Avaya **strongly recommends** that a DHCP server be available at remote sites if WAN failures isolate IP telephones from the central site DHCP server(s).

The file server provides the 4600 Series IP Telephone with a script file and, if appropriate, new or updated application software. See Step 3: Telephone and File Server on page 36 under Initialization Process. In addition, you can edit an associated settings file to customize telephone parameters for your specific environment. See Administering Options for the 4600 Series IP Telephones on page 96.

H.323

Registration and Authentication

The Avaya Media Server supports using the extension and password to register and authenticate 4600 Series IP Telephones. For further information, see Related Documents on page 18.

SIP

Registration and Authentication

A 4600 Series SIP IP Telephone requires an off-PBX station (OPS) extension on the Avaya Communication Manager and a login and password on the Registration Server to register and authenticate it. Registration is described in the Initialization process, in Step 4: Telephone and the Call Server on page 37. For further information, see the *Converged Communication Server Release 3.0 Installation and Administration Guide* (555-245-705), available on the Avaya support Web site, http://www.avaya.com/support.

WAN Considerations

QoS is harder on a WAN than a LAN. A LAN assumes no bandwidth concerns. A WAN assumes a finite amount of bandwidth. Therefore, QoS considerations are more significant when the IP telephony environment includes a WAN. In addition, there are administrative and hardware compatibility issues unique to WANs. WAN administration is beyond the scope of this document.

Initialization Process

These steps offer a high-level description of the information exchanged when the telephone initializes and registers. This description assumes that all equipment is properly administered ahead of time. This description can help you understand how the 4600 Series IP Telephones relate to the routers and servers in your network.

Step 1: Telephone to Network

The telephone is appropriately installed and powered. After a short initialization process, the telephone identifies the LAN speed. If applicable to your network and telephone model, 802.1X Supplicant authentication occurs at this time, where an 802.1X ID and password have to be submitted to proceed. Then the telephone sends a DHCP message out into the network, identifying itself and requesting further information. Depending on your network structure, the message goes directly to the DHCP server or a network router receives the message and relays it to the appropriate DHCP server.

Step 2: DHCP Server to Telephone

The DHCP file server provides information to the telephone, as described in DHCP and File Servers on page 56. Among other data passed to the telephone is the IP Address of the TFTP or HTTP server, which is crucial for the next step.

Step 3: Telephone and File Server

Many 4600 Series IP Telephones can download script files, application files, and settings files from either a TFTP, HTTP, or HTTPS server. For specific telephone/server compatibility, see Table 1. If you have a mixture of telephones, you can use either:

- TFTP servers only.
- Both TFTP and HTTP servers, with TFTP running telephones with older releases and HTTP for telephones capable of using HTTP.

You need TFTP servers for upgrades if you have a release prior to R2.2 on a telephone. Currently, only Avaya servers support 4600 Series IP Telephone file transfers using HTTPS. The reason is 4600 Series IP Telephones only establish encrypted TLS connections with servers that use Avaya-signed digital certificates.

A telephone that supports HTTP will attempt to access the HTTP server (if administered), and, if successful, will not attempt to access the TFTP server (if administered).

The script files, application files, and settings files discussed in this section are identical for HTTP and TFTP servers. The general downloading process for those files is essentially the same. One exception is that when you use an HTTPS server, a TLS server is contacted first. Therefore, we use the generic term “file server” here to mean both “TFTP server” and “HTTP server.”

The telephone queries the file server, which transmits a script file to the telephone. This script file, at a minimum, tells the telephone which application file the telephone must use. The application file is the software that has the telephony functionality, and can be easily updated for future enhancements.

The telephone uses the script file to determine if it has the proper application file. A newly installed telephone may have no application file, and therefore would not have the proper one. A previously installed telephone might not have the proper application file. If the telephone determines the application file indicated in the script file is missing, the telephone requests a download of the proper application file from the file server. The file server then downloads the file and conducts some checks to ensure that the file was downloaded properly. If the telephone determines it already has the proper file, the telephone proceeds to the next step without downloading the application file again.

After checking and loading the application file, the 4600 Series IP Telephone, if appropriate, uses the script file to look for a settings file. The settings file can contain options you have administered for any or all of the 4600 Series IP Telephones in your network. For more information about this settings file, see Administering Options for the 4600 Series IP Telephones on page 96.

Step 4: Telephone and the Call Server

The call server referred to in this step differs depending on whether the telephone is H.323 or SIP. For H.323 IP telephones, the call server is the Avaya Media Server. For SIP IP telephones, the call server is the Registration Server.

In this step, the telephone and the call server exchange a series of messages, which cause the display on the telephone to prompt the user. For a new installation and for full service, the user must enter the telephone’s extension and the call server password. For a restart of an existing installation, this information is already stored on the telephone, but the user may have to confirm the information. The telephone and the call server exchange more messaging, with the expected result being that the telephone is appropriately registered.

An exception to the requirement to enter an extension and password is for H.323 IP telephones running R2.3 and later software. These telephones support a feature called Unnamed Registration. Unnamed Registration allows a telephone to register with the Avaya Media Server without an extension, assuming the Avaya Media Server also supports this feature. To invoke Unnamed Registration, take no action—just let the **Extension...** prompt display for 60 seconds without making an entry. The telephone will automatically attempt to register by means of

Unnamed Registration. A telephone registered with Unnamed Registration has the following characteristics:

- only one call appearance,
- no administrable features,
- can make only outgoing calls, subject to call server Class of Restriction/Class of Service limitations, and
- can be converted to normal “named” registration by entering a valid extension and password.

More details about the installation process are available in the *4600 Series IP Telephone Installation Guide* and in Chapter 3: Requirements of this document.

TCP/UDP Port Utilization

Like most network equipment, the 4600 Series IP Telephones use a variety of protocols, particularly TCP and UDP, to communicate with other equipment in that network—numerous different types of servers, routers, other telephones, etc. Part of this communication identifies which TCP and/or UDP ports each piece of equipment uses to support each protocol and each task within the protocol.

Depending on your network, you might need to know what ports or ranges are used in the 4600 Series IP Telephones’ operation. Knowing these ports or ranges allows you to appropriately administer your networking infrastructure. In this case, you will find the following material useful.

In Figure 1, Figure 2, and Figure 3:

- The box on the left always represents the 4600 Series IP Telephone.
- Depending on the diagram, the boxes on the right refer to various pieces of network equipment with which the telephone can (or will) communicate.
- Open-headed arrows (for example, ⟶) represent the direction(s) of socket initialization.
- Closed-headed arrows (for example, ⟷) represent the direction(s) of data transfer.
- The text the arrows point to identifies the port or ports that the 4600 Series IP Telephones support for the specific situation. Brackets identify ranges when more than one port applies. In addition, the text indicates any additional qualifications or clarifications. In many cases, the ports used are the ones called for by IETF or other standards bodies.
- Many of the diagrams’ explanations refer to system parameters or options settings, for example, IRSTAT or DIRSRVR. See Administering Options for the 4600 Series IP Telephones in Chapter 4: Server Administration for more information on parameters and settings.

Figure 1: Signaling, Audio and Management Diagram

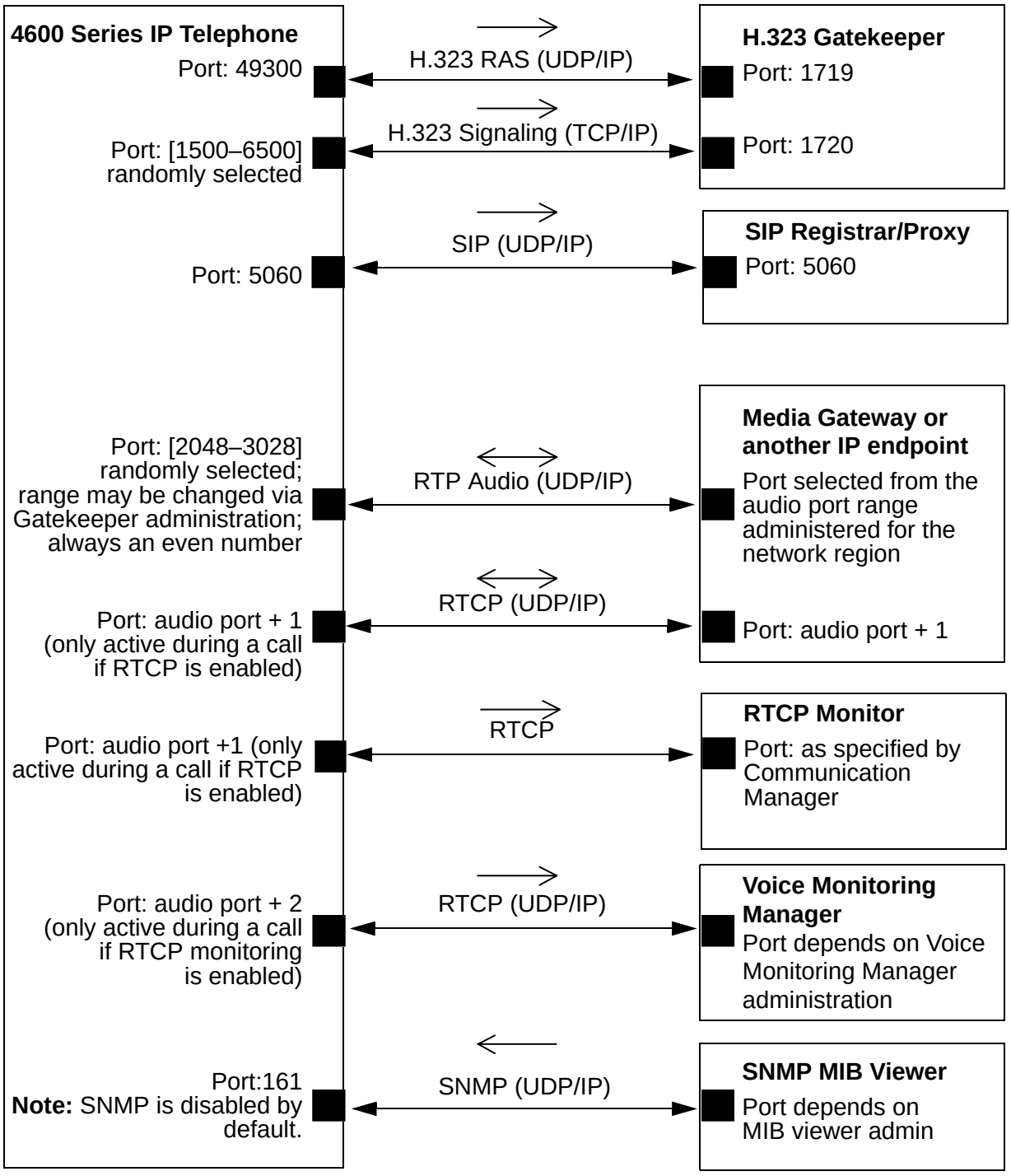

Signaling, Audio and Management
4600 Series IP Telephone
Port: 49300
Port: [1500–6500] randomly selected
Port: 5060
Port: [2048–3028] randomly selected; range may be changed via Gatekeeper administration; always an even number
Port: audio port + 1 (only active during a call if RTCP is enabled)
Port: audio port +1 (only active during a call if RTCP is enabled)
Port: audio port + 2 (only active during a call if RTCP monitoring is enabled)
Port:161
Note: SNMP is disabled by default.
H.323 RAS (UDP/IP)
H.323 Signaling (TCP/IP)
SIP (UDP/IP)
RTP Audio (UDP/IP)
RTCP (UDP/IP)
RTCP
RTCP (UDP/IP)
SNMP (UDP/IP)
H.323 Gatekeeper
Port: 1719
Port: 1720
SIP Registrar/Proxy
Port: 5060
Media Gateway or another IP endpoint
Port selected from the audio port range administered for the network region
Port: audio port + 1
RTCP Monitor
Port: as specified by Communication Manager
Voice Monitoring Manager
Port depends on Voice Monitoring Manager administration
SNMP MIB Viewer
Port depends on MIB viewer admin

Figure 2: Initialization and Address Resolution Diagram

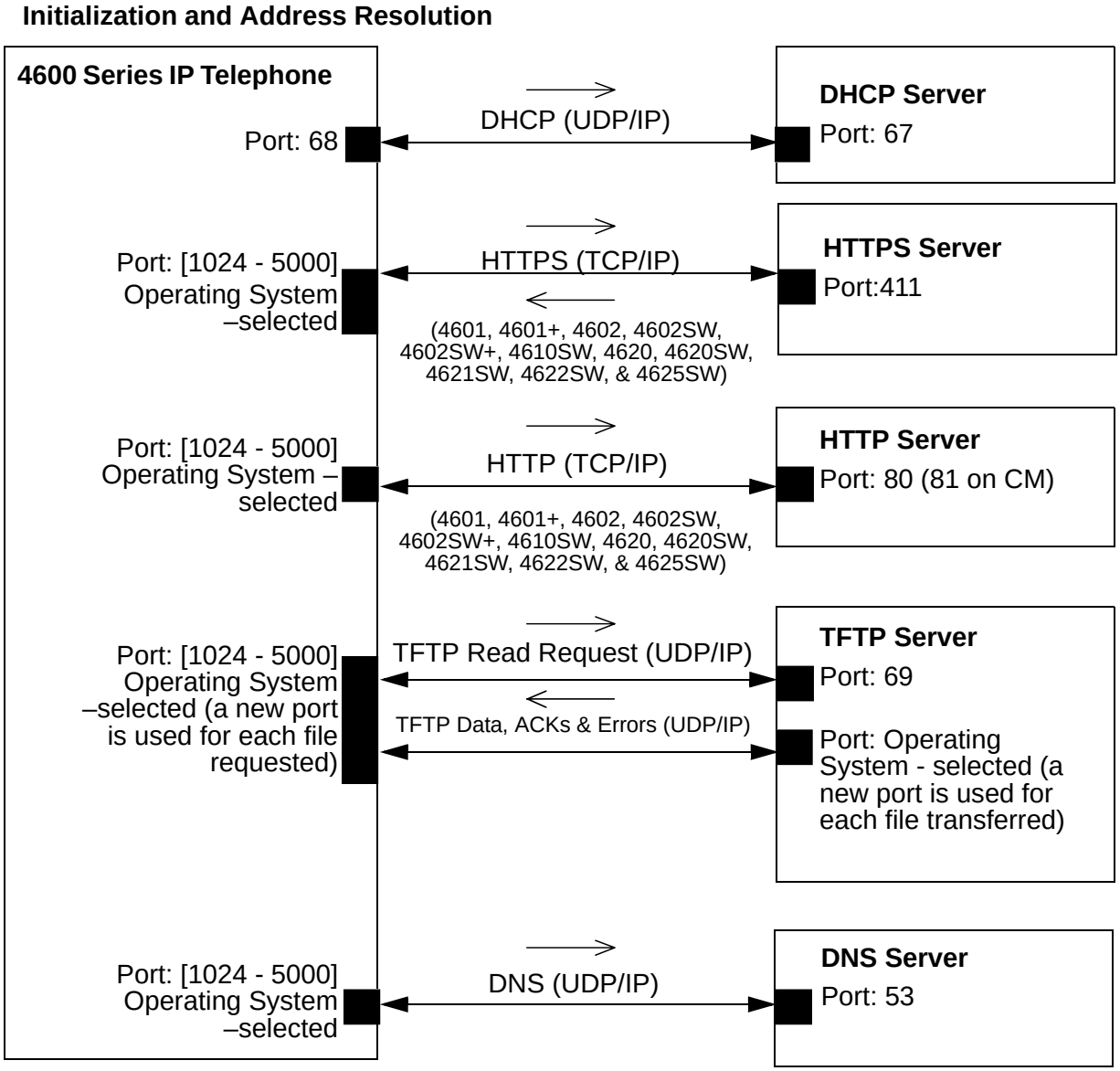
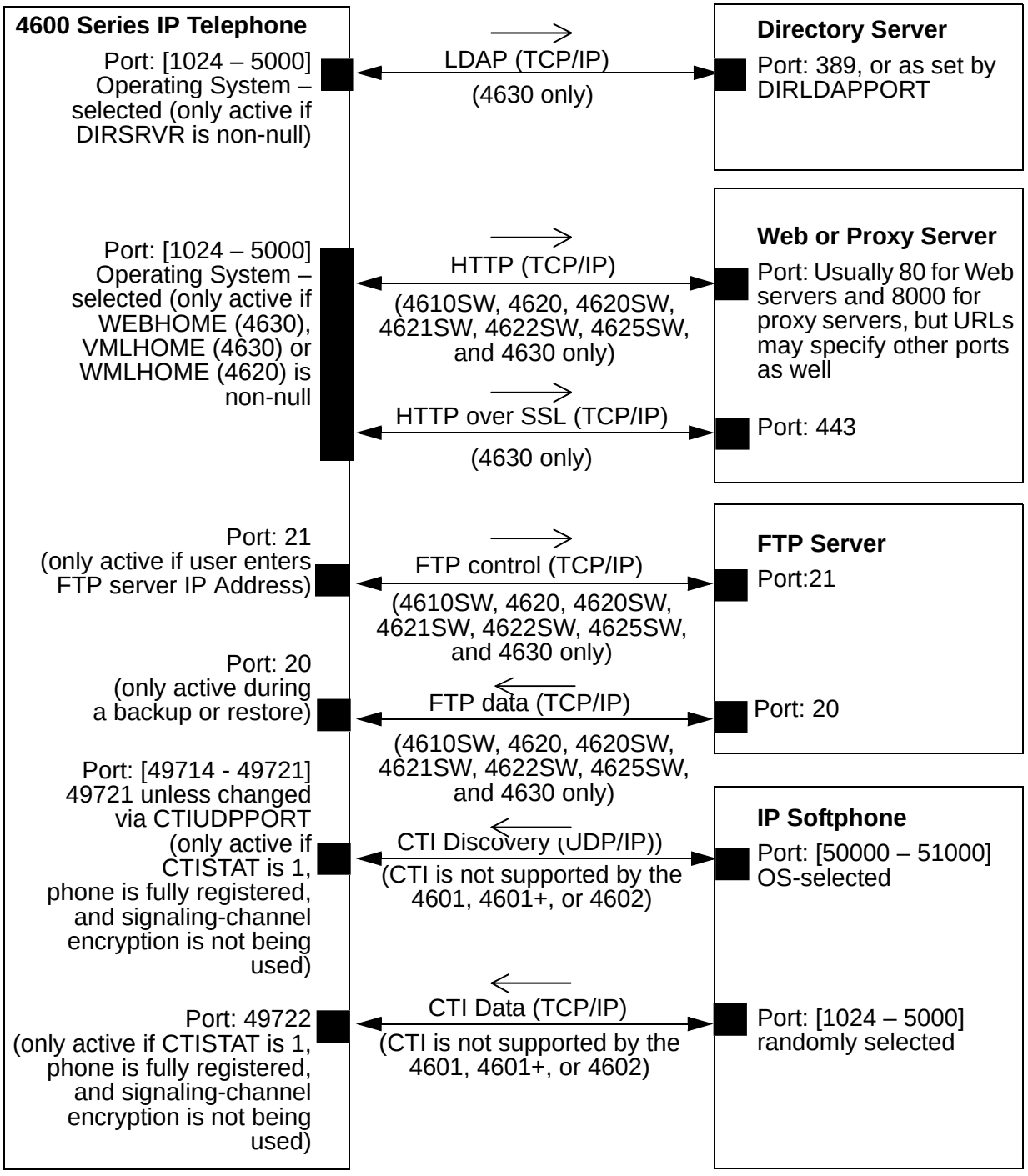
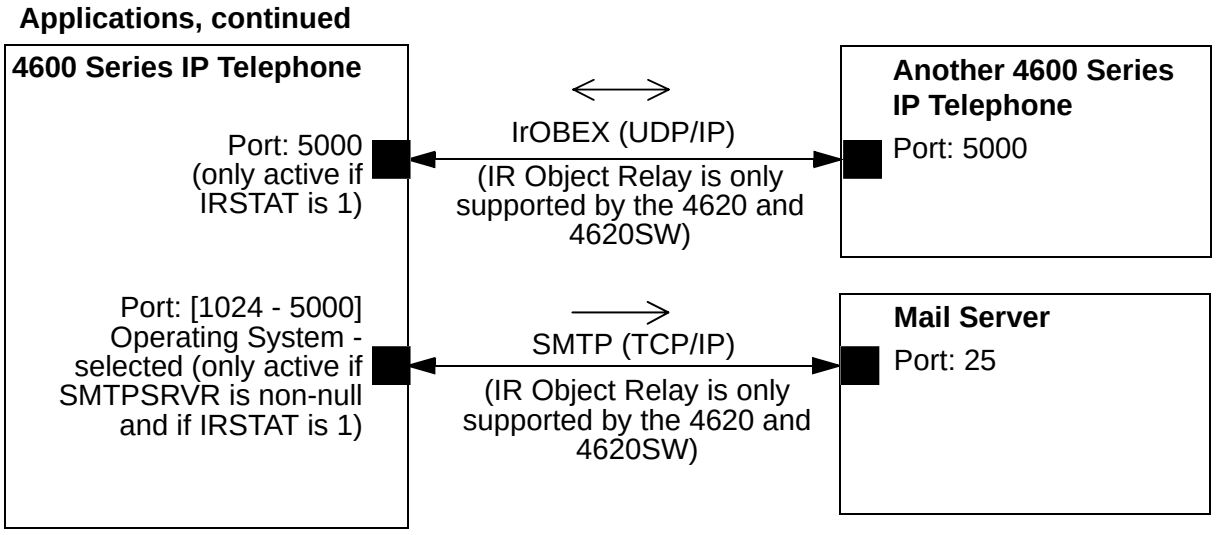

Initialization and Address Resolution
4600 Series IP Telephone
Port: 68
DHCP (UDP/IP)
DHCP Server
Port: 67
Port: [1024 - 5000] Operating System –selected
HTTPS (TCP/IP)
(4601, 4601+, 4602, 4602SW, 4602SW+, 4610SW, 4620, 4620SW, 4621SW, 4622SW, & 4625SW)
HTTPS Server
Port:411
Port: [1024 - 5000] Operating System – selected
HTTP (TCP/IP)
(4601, 4601+, 4602, 4602SW, 4602SW+, 4610SW, 4620, 4620SW, 4621SW, 4622SW, & 4625SW)
HTTP Server
Port: 80 (81 on CM)
Port: [1024 - 5000] Operating System –selected (a new port is used for each file requested)
TFTP Read Request (UDP/IP)
TFTP Data, ACKs & Errors (UDP/IP)
TFTP Server
Port: 69
Port: Operating System - selected (a new port is used for each file transferred)
Port: [1024 - 5000] Operating System –selected
DNS (UDP/IP)
DNS Server
Port: 53

Figure 3: Applications Diagram


Applications
4600 Series IP Telephone
Port: [1024 – 5000] Operating System – selected (only active if DIRSRVR is non-null)
LDAP (TCP/IP)
(4630 only)
Directory Server
Port: 389, or as set by DIRLDAPPORT
Port: [1024 – 5000] Operating System – selected (only active if WEBHOME (4630), VMLHOME (4630) or WMLHOME (4620) is non-null
HTTP (TCP/IP)
(4610SW, 4620, 4620SW, 4621SW, 4622SW, 4625SW, and 4630 only)
HTTP over SSL (TCP/IP)
(4630 only)
Web or Proxy Server
Port: Usually 80 for Web servers and 8000 for proxy servers, but URLs may specify other ports as well
Port: 443
Port: 21 (only active if user enters FTP server IP Address)
FTP control (TCP/IP)
(4610SW, 4620, 4620SW, 4621SW, 4622SW, 4625SW, and 4630 only)
FTP Server
Port:21
Port: 20 (only active during a backup or restore)
FTP data (TCP/IP)
(4610SW, 4620, 4620SW, 4621SW, 4622SW, 4625SW, and 4630 only)
Port: 20
Port: [49714 - 49721] 49721 unless changed via CTIUDPPORT (only active if CTISTAT is 1, phone is fully registered, and signaling-channel encryption is not being used)
CTI Discovery (UDP/IP))
(CTI is not supported by the 4601, 4601+, or 4602)
IP Softphone
Port: [50000 – 51000] OS-selected
Port: 49722 (only active if CTISTAT is 1, phone is fully registered, and signaling-channel encryption is not being used)
CTI Data (TCP/IP)
(CTI is not supported by the 4601, 4601+, or 4602)
Port: [1024 – 5000] randomly selected



Suggestions for Installation and Configuration

Reliability and Performance

There is a cost/performance trade-off associated with Voice over IP. Greater reliability and improved performance can be obtained through server redundancy and components with higher bandwidth capabilities.

The reliability and performance of the traditional PBX systems are very high to date. Much of the LAN is outside the PBX's control. However, consider the points in the next paragraph to enhance the reliability and performance of the IP telephone network.

All 4600 Series IP Telephones support the tools "ping" and "traceroute." These are standard LAN/WAN tools to identify:

- whether two points on a network can communicate with each other, and
- what path a sample communication takes as it traverses the network from one point to the other.

All 4600 Series IP Telephones respond appropriately to a ping or a traceroute message sent from the DEFINITY® or MultiVantage™ switch or any other source on your network. These telephones will not, in general, initiate a ping or traceroute. Release 1.6 of the 4600 Series IP Telephones supporting H.323 introduced "remote ping" and "remote traceroute" support. The

switch can instruct such a 4600 Series IP Telephone to initiate a ping or a traceroute to a specified IP Address. The telephone carries out that instruction and sends a message to the switch indicating the results. See your DEFINITY® or MultiVantage™ Administration documentation for more details.

As of Release 1.8, if applicable, 4600 Series IP Telephones test whether the network Ethernet switch port supports IEEE 802.1D/q tagged frames by ARPing the router with a tagged frame. See VLAN Considerations on page 86. If your LAN environment includes Virtual LANs (VLANs), your router must respond to ARPs for VLAN tagging to work properly.

IP Address Lists and Station Number Portability

Release 1.5 of the 4600 Series IP Telephones provided the capability to specify IP Address lists in either dotted decimal or DNS format. Release 1.5 allowed key network elements to have multiple IP Addresses, rather than being restricted to just one address for each element. You can specify up to 127 total characters in each list of the following devices:

- router/gateways,
- DHCP/TFTP/HTTP servers, and
- the media server.

Upon startup or a reboot, the 4600 Telephone attempts to establish communication with these various network elements in turn. The telephone starts with the first address on the respective list. If the communication is denied or times out, the telephone proceeds to the next address on the appropriate list and tries that one. The telephone does not report failure unless all the addresses on a given list fail.

Obviously, this capability significantly improves the reliability of IP telephony. Multiple IP Addresses maximize the telephone's likelihood to communicate with backup equipment if the primary equipment is not operating or is not accessible. For example, alternate communication would be needed during a limited network outage.

However, this capability also has the advantage of making station number portability easier. Assume a situation where the company has multiple locations in London and New York, all sharing a corporate IP network. Users want to take their telephones from their offices in London and bring them to New York. When users start up their telephones in the new location, the local DHCP server will generally route them to the local call server. In this case the call server for H.323 is the Avaya Media Server and the call server for SIP is the Registration Server. But the local call server denies service because it knows nothing about these new users. With proper administration of the local DHCP server, the telephone knows to try a second call server IP Address, this one in London. The user can then be automatically registered with the London call server.

Chapter 4: Server Administration contains details on administration of DHCP servers for lists of alternate media servers, router/gateways, and TFTP servers. For specific information, see DNS Addressing on page 107.

Security

In VoIP, physical wire is replaced with an IP connection. The connection is more mobile. Unauthorized relocation of the IP telephone allows unauthorized users to send and receive calls as the valid owner. For further details on toll fraud, see the DEFINITY® or Avaya Communication Manager documents mentioned in Related Documents on page 18.

Any equipment on a data network, including a 4600 Series IP Telephone, can be the target of a Denial of Service attack. Usually, such an attack consists of flooding the network with so many messages that the equipment either:

- spends so much time processing the messages that legitimate tasks are not processed, or
- the equipment overloads and fails.

The 4600 Series IP Telephones cannot guarantee resistance to all Denial of Service attacks. However, each Release has increasing checks and protections to resist such attacks while maintaining appropriate service to legitimate users.

All 4600 Series IP Telephones that have WML Web applications and run R2.2 or greater software support Transport Layer Security (TLS). This standard allows the telephone to establish a secure connection to a HTTPS server, in which the telephone's upgrade and settings file can reside. This setup adds security over the TFTP alternative.

You also have a variety of optional capabilities to restrict or remove how crucial network information is displayed or used. These capabilities are covered in more detail in Chapter 4: Server Administration, and include:

- As of Release 2.7, the 4602SW+ and 4625SW IP Telephones support IEEE 802.1X as a Supplicant with the EAP-MD5 authentication method. The functionality is identical to other 4600 Series SW IP Telephones supporting this feature.
- As of Release 2.6, SNMP is disabled by default. You must enable SNMP through DHCP or the 46xxsettings file.
- As of Release 2.6, the 4610SW, 4620SW, 4621SW, and 4622SW IP Telephones support IEEE 802.1X as a Supplicant with the EAP-MD5 authentication method. The modes supported are as follows:
  - Unicast Supplicant operation only with PAE multicast pass-through, with and without proxy Logoff, and
  - Unicast or multicast Supplicant operation without PAE multicast pass-through or proxy Logoff.

  Note:

  The 4601 and 4601+ IP Telephones do not support 802.1X as a Supplicant.

- As of Release 2.3, 4600 Series H.323 IP Telephones support signaling channel encryption while registering, and when registered, with appropriately administered Avaya Media Servers.
- As of Release 2.0, a 4600 Series IP Telephone's response to SNMP queries is restricted to only IP Addresses on a list you specify.
- As of Release 2.0, an SNMP community string is specified for all SNMP messages sent by the telephone.
- As of Release 1.8, dialpad access to Local Administration Procedures, such as specifying IP Addresses, is restricted by a password.
- Dialpad access to most Local Administration Procedures was removed.
- The end user's ability to use a telephone Options application to view network data is restricted.

Chapter 3: Requirements

Introduction

The 4600 Series IP Telephones use Internet Protocol (IP) technology with Ethernet line interfaces. The IP telephones supplement the existing Avaya IP Solutions platform. This feature provides the user with the capability to natively administer and maintain new 4600 Series IP Telephones.

The 4600 Series IP Telephones provide support for DHCP, TFTP, and HTTP over IPv4/UDP, which enhance the administration and servicing of the phones. These phones use DHCP to obtain dynamic IP Addresses and TFTP or HTTP to download new versions of software for the phones.

Using either a built-in hub or a switched port, the 4600 Series IP Telephones offer one desktop connection for both the telephone set and the PC.

Note:

In all cases, references to “Avaya Communication Manager” or “CM” apply only to 4600 Series IP Telephones supporting H.323.

Hardware Requirements

Before plugging in the 4600 Series IP Telephone, verify that all the hardware requirements are met. Failure to do so prevents the telephone from working and might have a negative impact on your network.

The following hardware is required for 4600 Series IP Telephones supporting H.323 to work properly.

Note:

The recommended configuration is the latest PBX software and the latest IP telephone firmware. In the event your site does not have the latest PBX software, follow the recommendations in the table immediately following.

Media Server Release (H.323 only)	Avaya IP Telephone	IP Telephone Release	Notes
Avaya Communication Manager 3.1	4601+, 4602+, and 4625SW	R2.7	
Avaya Communication Manager 3.0	All telephones except 4601, 4602, 4602SW, and 4625SW	R2.6	
Avaya Communication Manager 1.3+	All telephones	R1.8+	Use the latest release.
Avaya Communication Manager 1.1, Avaya Communication Manager 1.2	All telephones *except* 4630	R1.8+	Use the latest release.
R10, Avaya Communication Manager 1.1, Avaya Communication Manager 1.2	4630	R1.74	Upgrade to Avaya Communication Manager Release 1.3 or later before installing R1.8 on 4630 Telephones.
R10	4606, 4612, 4624	R1.8+	The 4602 and 4620 are not supported.
R9.5	4606, 4612, 4624	R1.8+	The 4620, 4602, and 4630 are not supported. R1.5 is the minimum 4600 IP Telephone vintage.
R9	4612, 4624	R1.1	R1.1 is the only supported 4600 IP Telephone vintage.
R8.4	4612, 4624	R1.0	R1.0 is the only supported 4600 IP Telephone vintage.

4600 Series IP Telephones supporting SIP need Avaya Converged Communications Server (CCS) Release 3.0, which includes SIP Enablement Services (SES), to work properly. Avaya Communication Manager is considered a “feature server” behind SES that provides Off-PBX Station (OPS) features.

Additional Hardware Requirements

- Ensure that the appropriate circuit pack(s) are administered on your media server. See the media server's hardware guide for more detail.

  Important:

  IP telephone firmware Release 2.3 or greater requires TN799C V3 or greater Control-LAN (C-LAN) circuit pack(s). For more information, see the *Communication Manager Software and Firmware Compatibility Matrix* on the Avaya support Web site http://www.avaya.com/support.

- A Category 5e LAN. If the telephones are to be powered from the LAN, the power supply must be designed to the IEEE 802.3af-2003 standard for LAN powering.
- Electrical power provided to each telephone by one of the following two sources:
  - A Telephone Power Module, also called the DC power jack. You must order this module separately, except for the 4630 and the 4690 phones. The 4630 comes with its own power brick and the 4690 has its own power interface module. The 4630SW does not come with a power brick. For the 4630SW, you must order the power brick separately if LAN powering will not be used for that particular telephone model.
  - IEEE 802.3af-2003, if the LAN supports this powering scheme. Note that the 4630 and 4690 **cannot** be powered this way, but the 4630SW **can** be powered this way.
- Verify that the 4600 Series IP Telephone package includes the following components:
  - 1 telephone set.
  - 1 telephone handset. Note that the 4622SW and the 4690 telephones do not come with handsets.
  - 1 H4DU 4-conductor coiled handset cord that is 9 feet long when extended, plugged into the telephone and the handset. The handset cord for the 4601 and 4601+ is 6 feet long. Not applicable for the 4622SW and 4690 IP Conference Telephones.
  - 1 Category 5 modular line cord for the connection from the IP telephone to the Ethernet wall jack.
  - *4600 Series IP Telephone Safety Instructions* (555-233-779).
  - Power Interface Module for the 4690 IP Conference Telephone only.
  - Power Brick for 4630 IP Telephones only.
  - Stylus for 4630/4630SW IP Telephones only.
- You might need a Category 5e modular line cord for the connection from the 4600 Series IP Telephone to the PC.

  Note:

  See the *4600 Series IP Telephone Installation Guide*.

Software Requirements

The following software is required for 4600 Series IP Telephones to work properly:

- The DHCP server and application must be installed and properly administered, as described in DHCP on page 58.

  CAUTION:

  A DHCP server is not mandatory, but static addressing is necessary when a DHCP server is unavailable. Because of difficulties associated with static addressing, we **very strongly recommend** that a DHCP server be installed and that static addressing be avoided.

- The TFTP and/or HTTP file server and application must be properly administered, as described in TFTP (H.323 Only) on page 71 and HTTP on page 73.

  CAUTION:

  A file server does not need to be available for the Avaya IP Telephones to operate. The Avaya IP Telephones obtain important information from the script files on the file server and depend on the application file for software upgrades. If the file server is not available when the Avaya IP Telephones reset, the telephones will register with the media server and operate. Some features may not be available, and restoring those features requires resetting the Avaya IP Telephone(s) when the file server is available.

- For 4630 and 4630SW IP Telephone environments, if users are to have access to LDAP directories or corporate Web sites, the appropriate servers must be in place. The 4630/4630SW Telephones must be appropriately administered in accordance with Server Administration on page 51.

  CAUTION:

  4630 IP Telephone Release 1.72 introduced significant software architecture changes. Thus, unlike most 4600 Series IP Telephones software releases, 4630 IP Telephone Release 1.72 and later **cannot** be downgraded to a release earlier than 1.72. Attempting to do so renders the 4630 (and 4630SW, if Release 1.8 or greater) set inoperable. In addition, if you are upgrading a 4630 from a release prior to Release 1.61, you must first upgrade to Release 1.61. Then you must upgrade to the newer Release. You **cannot** upgrade directly from a pre-1.61 Release to a post-1.61 Release for the 4630.

- For 4610SW/4620/4620SW/4621SW/4622SW/4625SW IP Telephone environments, if users are to have access to LDAP directories or corporate WML Web sites, the appropriate servers must be in place. You must download the LDAP Directory Application software from the Avaya support Web site. You must appropriately administer the telephones in accordance with Server Administration on page 51.

  Note:

  Ensure that all required parameters are configured correctly. For Avaya Media Server information, see your administration documentation. For the DHCP and file servers, see Chapter 4: Server Administration.

Chapter 4: Server Administration

Introduction

When a 4600 Series IP Telephone is plugged in and powered, it automatically negotiates with its associated LAN to determine the Ethernet speed. From that point on, the telephone's actions depend largely on network administration prior to telephone installation, and on any actions the installer takes. This chapter details the parameters and other data the telephone needs to operate, and the alternatives to deliver that information to the telephone, where appropriate. Recommendations and specifications for alternatives to certain parameters are also provided.

The parameters under which the telephone needs to operate are summarized as follows:

- Telephone Administration on the call server. The call server for H.323 is the Avaya Media Server, while the call server for SIP is the Registration Server.
- IP Address management for the telephone.
- Tagging Control and VLAN administration for the telephone, if appropriate.
- Quality of Service (QoS) administration for the telephone, if appropriate.
- Site-specific Option Number (SSON) setting of DHCP servers, if appropriate.
- Protocol administration, for example, Simple Network Management Control (SNMP) and Link Layer Discovery Protocol (LLDP).
- Interface administration for the telephone, if appropriate.
- Application-specific telephone administration, if appropriate. For example, Directory- or Web-specific information required for these optional applications.

The delivery mechanisms are:

- Maintaining the information on the call server.
- Manually entering the information using the telephone dialpad.
- Administering the DHCP server.
- Editing the settings file on the applicable TFTP or HTTP file server.

These parameters can be administered in a variety of ways, as indicated in Table 2. Note that not all parameters can be administered on all delivery mechanisms.

Table 2: Administration Alternatives and Options for 4600 Series IP Telephones

Parameter(s)	Administrative Mechanisms	For More Information See:
Telephone Administration	Avaya call server (applies only to H.323)	Administering 4600 Series IP Telephones on Avaya Media Servers (H.323 Only) on page 55 and Related Documents on page 18.
IP Addresses	DHCP (strongly recommended)	DHCP and File Servers on page 56, and especially DHCP on page 58.
	Manual administration at the telephone	"Static Addressing Installation" in Chapter 3 of the *4600 IP Telephone Installation Guide.*
Tagging and VLAN	LLDP	See Link Layer Discovery Protocol (LLDP) on page 92.
	DHCP	DHCP and File Servers on page 56, and Administering Options for the 4600 Series IP Telephones on page 96. Also see VLAN Considerations on page 86 for background information.
	Settings file (strongly recommended)	DHCP and File Servers on page 56 and Administering Options for the 4600 Series IP Telephones on page 96.
	Manual administration at the telephone	"Static Addressing Installation" in Chapter 3 of the *4600 IP Telephone Installation Guide*.
Quality of Service	Avaya call server (applies only to H.323)	Administering 4600 Series IP Telephones on Avaya Media Servers (H.323 Only) on page 55 and Related Documents on page 18.
	DHCP	DHCP and File Servers on page 56, and Administering Options for the 4600 Series IP Telephones on page 96.
	Settings file (strongly recommended)	DHCP and File Servers on page 56, and Administering Options for the 4600 Series IP Telephones on page 96.
	Manual administration at the telephone	See "QoS Option Setting" in Chapter 3 of the *4600 IP Telephone Installation Guide*.
Interface	DHCP	DHCP and File Servers on page 56, and Administering Options for the 4600 Series IP Telephones on page 96.
	Settings file (strongly recommended)	DHCP and File Servers on page 56, and Administering Options for the 4600 Series IP Telephones on page 96.
	Manual administration at the telephone	See "Secondary Ethernet (Hub) Interface Enable/Disable" in Chapter 3 of the *4600 IP Telephone Installation Guide*.

1 of 2

Table 2: Administration Alternatives and Options for 4600 Series IP Telephones (continued)

Parameter(s)	Administrative Mechanisms	For More Information See:
SSON	DHCP	Customizing the Site-Specific Option Number (SSON) on page 108. DHCP and File Servers on page 56, and especially DHCP on page 58.
	Settings file (strongly recommended)	Customizing the Site-Specific Option Number (SSON) on page 108. DHCP and File Servers on page 56, and especially TFTP Generic Setup on page 72 and HTTP Generic Setup on page 73.
	Manual administration at the telephone	"Site-Specific Option Number Setting" in Chapter 3 of the *4600 IP Telephone Installation Guide*.
802.1X	DHCP	IEEE 802.1X on page 90.
	Settings file	IEEE 802.1X on page 90.
	Manual administration at the telephone	"802.1X Supplicant Authentication" and "Set the 802.1X Operational Mode" in the *4600 Series IP Telephone Installation Guide.*
SNMP	DHCP	DHCP on page 58.
	Settings file	4600 Series IP Telephone Scripts and Application Files on page 74 and 4600 Series IP Telephone Customizable System Parameters on page 96.
Application - specific parameters	DHCP	DHCP and File Servers on page 56, and especially DHCP on page 58. Also, Customizing the 4630/4630SW IP Telephone on page 111 and Customizing 4610SW, 4620/4620SW, 4621SW, 4622SW, and 4625SW IP Telephones on page 116.
	Settings file (strongly recommended)	DHCP and File Servers on page 56, especially TFTP (H.323 Only) on page 71. Also, Customizing the 4630/4630SW IP Telephone on page 111 and Customizing 4610SW, 4620/4620SW, 4621SW, 4622SW, and 4625SW IP Telephones on page 116.
	LLDP	Link Layer Discovery Protocol (LLDP) on page 92.

2 of 2

General information about administering DHCP servers is covered in DHCP and File Servers on page 56, and more specifically, DHCP on page 58. General information about administering TFTP servers is covered in DHCP and File Servers, and more specifically, TFTP (H.323 Only) on page 71. General information about administering HTTP servers is covered in DHCP and File Servers, and more specifically, HTTP. Once you are familiar with that material, you can administer telephone options as described in Administering Options for the 4600 Series IP Telephones on page 96.

Parameter Data Precedence

If a given parameter is administered in multiple places, the last server to provide the parameter has precedence. The precedence, from lowest to highest, is:

- LLDP
- manual administration, with the two exceptions described for the system parameter STATIC on page 106.
- DHCP,
- TFTP/HTTP,
- the call server (meaning the Avaya Media Server for H.323, and the Registration Server for SIP), and finally,
- FTP backup files (if administered and if permitted).

Settings the IP telephone receives from backup files or the media server overwrite any previous settings including manual settings. The only exception to this sequence is in the case of VLAN IDs. In the case of VLAN IDs, LLDP settings of VLAN IDs are the absolute authority. Then the usual sequence applies through TFTP or HTTP as appropriate. If the VLAN ID is not zero, any VLAN ID from the media server is ignored.

Administering H.323 and SIP IP Telephones on the Same Network

Both H.323- and SIP-based telephones can run on the same LAN or VLAN without difficulty. You can even mix H.323 phones and SIP phones having the same model, for example, the 4620SW. However, any given telephone supports only one signaling protocol at a time. You must therefore ensure that the proper application files (the software that runs in the telephone) are sent to the appropriate telephones. For information on downloading the software to the telephones, see Choosing the Right Application File and Upgrade Script File later in this chapter.

In general, H.323 and SIP telephones use the same administration mechanisms, with the exception that H.323 phones get some telephony administration from the Avaya call server. If you intend to mix H.323 and SIP telephones on the same network, you can use common information in either DHCP or in a common script file for those settings common to both types of sets. Because settings not applicable to a given telephone set are ignored, you can send SIP-specific settings to an H.323 telephone and H.323 settings to a SIP telephone without creating problems.

Administering 4600 Series IP Telephones on Avaya Media Servers (H.323 Only)

DEFINITY Releases 9, 9.5, 10, and Avaya Communication Manager Software Release 1.1+

DEFINITY® Releases 9 and 9.5 provide support for the 4606, 4612, and 4624 IP Telephones. DEFINITY® Release 10 adds support for the 4630 and 4630SW IP Telephones. Avaya Communication Manager Software Release 1.1 adds support for the 4602/4602SW and 4620/4620SW IP Telephones. Avaya Communication Manager 3.1 supports the 4601+ and 4602SW+ IP Telephones. Administration of a 4612 and 4624 IP Telephone is identical to a 6424 IP softphone. The 4610SW and 4690 are not natively supported, but can be aliased as 4620 IP Telephones. See Related Documents on page 18, particularly the *Administration for Network Connectivity* and the *Administrator Guides*. Follow these guidelines:

- On the Customer Options form, verify that the **IP Stations** field is set to "**y**" (Yes). If it is not, contact your Avaya sales representative.
- The **IP Softphone** field does not have to be set to "**y**" (Yes).

DEFINITY Release 8.4

Note:

DEFINITY® Release 8.4 is very old. We do not recommend using this release.

DEFINITY® Release 8.4 supports the 4612 and 4624 IP Telephones. The 4612 and 4624 IP Telephones are aliased as 6424 Telephones, administered as IP Softphones. The administrative forms for the 6424 IP Softphone are used for the two IP telephones. See Related Documents on page 18, particularly the *Administration for Network Connectivity* and the *Administrator Guides*. Follow these guidelines:

- Alias the IP telephone as a 6424D+ DCP set, with the **IP Softphone** field set to "**y**" (Yes).
- Administer a **Media Complex Ext** for the audio channel.

DHCP and File Servers

Dynamic Host Configuration Protocol (DHCP) provides a means by which configuration parameters can be automatically assigned to clients on a TCP/IP network. DHCP minimizes a 4600 Series IP Telephone network's maintenance by removing the need to individually assign and maintain IP Addresses and other parameters for each IP telephone on the network.

Software Checklist

Ensure that you have purchased and/or own licenses to install and use any or all of the DHCP, TFTP, and HTTP server software.

Note:

It is possible to install the DHCP, TFTP, and HTTP server software on the same machine.

CAUTION:

The circuitry in the 4600 Series IP Telephones reserves IP Addresses of the form **192.168.2.x** for internal communications. The telephone(s) will not properly use addresses you specify if they are of that form.

Required Network Information

DHCP is the control point where an enterprise controls its IP telephones. Before administering DHCP and TFTP, HTTP, and TLS, as applicable, complete the information in Table 3: Required Network Information Before Installation - Per DHCP Server on page 57. Completing the pre-installation steps ensures that you have the necessary information regarding your network. If you have more than one Gateway, TFTP/HTTP/TLS server, subnet mask, and Gatekeeper in your configuration, you need to complete Table 3 for each DHCP server.

Release 1.5 of the 4600 Series Telephones supported specifying a list of IP Addresses for a gateway/router, TFTP server, and Avaya Media Server Gatekeeper(s). We explain this specification in Overview of Voice over IP (VoIP) on page 27. Each list can contain up to 255 total ASCII characters, with IP Addresses separated by commas with no intervening spaces. Note that depending on the specific DHCP application, only 127 characters might be supported.

When specifying IP Addresses for the file server or media server, use either dotted decimal format (“xxx.xxx.xxx.xxx”) or DNS names. If you use DNS, note that the system value DOMAIN is appended to the IP Addresses you specify. If DOMAIN is null, the DNS names must be fully qualified, in accordance with IETF RFCs 1034 and 1035. For more specific information about DNS, see DHCP Generic Setup on page 59 and DNS Addressing on page 107.

Table 3: Required Network Information Before Installation - Per DHCP Server

1. Gateway (router) IP Address(es)	
2. TFTP server IP Address(es)	H.323 only, if applicable.
3. Subnet mask	
4. Avaya Media Server Gatekeeper IP Address(es)	H.323 only.
5. Avaya Media Server Gatekeeper port	H.323 only. Although this can be a value between 0 and 65535, the default value is **1719**. Do not change the default value unless that value conflicts with an existing port assignment.
6. TFTP server file path	H.323 only, if applicable.
7. Telephone IP Address range *From*: *To*:	
8. DNS server address(es)	If applicable.
9. HTTP server address(es)	If applicable.
10. HTTPS/TLS server address(es)	If applicable.

The file server file path is the “root” directory the server uses for all transfers. This is the default directory all files will be uploaded to or downloaded from. In configurations where the upgrade script and application files are in the default directory, do not use item 6 in Table 3: Required Network Information Before Installation - Per DHCP Server on page 57.

DHCP

This section provides basic information on DHCP servers and generic information on DHCP server administration.

Choosing a DHCP Configuration

A discussion on how to best set up your network to work with the 4600 Series IP Telephones is beyond the scope of this document. See Network Assessment on page 32. This document concentrates on the simplest case of the single LAN segment. Information provided here can be extrapolated for more complex LAN configurations.

CAUTION:

Before you start, it is important that you understand your current network configuration. An improper installation can cause network failures or reduce the reliability and performance of your network.

DHCP Software Alternatives

Three DHCP software alternatives are common to Windows operating systems:

- Windows NT® 4.0 DHCP Server
- Windows 2000® DHCP Server
- Windows 2003® DHCP Server

Any other DHCP application might work. It is the customer's responsibility to install and configure the DHCP server correctly. This document is limited to describing a generic administration that works with the 4600 Series IP Telephones.

DHCP Generic Setup

This document is limited to describing a generic administration that works with the 4600 Series IP Telephones. Three DHCP software alternatives are common to Windows operating systems:

- Windows NT® 4.0 DHCP Server
- Windows 2003® DHCP Server
- Windows 2000® DHCP Server

Any other DHCP application might work. It is the responsibility of the customer to install and configure the DHCP server correctly.

DHCP server setup involves:

1. Installing the DHCP server software according to vendor instructions.
2. Configuring the DHCP server with:
   - IP Addresses available for the 4600 Series IP Telephones.
   - The following DHCP options:
     - **Option 1 - Subnet mask**.
       As described in Table 3, item 3.
     - **Option 3 - Gateway (router) IP Address(es)**.
       As described in Table 3, item 1. If using more than one address, the total list can contain up to 255 total ASCII characters. You must separate IP Addresses with commas with no intervening spaces.
     - **Option 6 - DNS server(s) address list**.
       If using more than one address, the total list can contain up to 127 total ASCII characters. You must separate IP Addresses with commas with no intervening spaces. At least one address in Option 6 must be a valid, non zero, dotted decimal address. Otherwise, DNS will fail.
     - **Option 15 - DNS Domain Name**.
       This string contains the domain name to be used when DNS names in system parameters are resolved into IP Addresses. This domain name is appended to the DNS name before the 4600 IP Telephone attempts to resolve the DNS address. Option 15 is necessary if you want to use a DNS name for the TFTP server. Otherwise, you can specify a DOMAIN as part of customizing TFTP as indicated in DNS Addressing on page 107.
     - **Option 51 - DHCP lease time**.
       Optional. Avaya recommends a lease time of six weeks or greater. Expired leases cause Avaya IP Telephones to reboot.Avaya recommends providing enough leases so an IP Address for an IP telephone does not change if it is briefly taken offline.

Note:

The DHCP standard states that when a DHCP lease expires, the device should immediately cease using its assigned IP Address. If the network has problems and the only DHCP server is centralized, the server is not accessible to the given telephone. In this case the telephone is not usable until the server can be reached.

Avaya recommends that, once assigned an IP Address, the telephone continues using that address after the DHCP lease expires, until a conflict with another device is detected. As Table 10: 4600 Series IP Telephone Customizable System Parameters indicates, the system parameter DHCPSTD allows an administrator to specify that the telephone will either:

- Comply with the DHCP standard by setting DHCPSTD to “1”, or
- Continue to use its IP Address after the DHCP lease expires by setting DHCPSTD to “0.”

The latter case is the default. If the default is invoked, after the DHCP lease expires the telephone sends an ARP Request for its own IP Address every five seconds. The request continues either forever, or until the telephone receives an ARP Reply. After receiving an ARP Reply, the telephone displays an error message, sets its IP Address to 0.0.0.0, and attempts to contact the DHCP server again.

- **Option 52 - Overload Option, if desired**.
  If this option is received in a message, the telephone interprets the **sname** and **file** fields in accordance with RFC 2132, Section 9.3.
- **Option 58 - DHCP lease renew time, if desired**.
  If not received or if this value is greater than that for Option 51, the default value of T1 (renewal timer) is used as per RFC 2131, Section 4.5.
- **Option 59 - DHCP lease rebind time, if desired**.
  If not received or if this value is greater than that for Option 51, the default value of T2 (rebinding timer) is used as per RFC 2131, Section 4.5.
- **Option 66 - TFTP Server Name**.
  Applicable to H.323 only.

Note:

Microsoft DHCP servers support only dotted-decimal format for file server addresses, not symbolic names. Option 66 need not be used if the TFTP server is identified in the Site Specific Option Number string (Option 176), or if HTTP is to be used exclusively instead of TFTP. However, to simplify configuration, Avaya recommends that you use Option 66 if you are using TFTP. If you use both Option 66 and Option 176 to identify TFTP servers, the value(s) in Option 176 overrides the value(s) in Option 66.

- A 4600 Series IP Telephone-specific DHCP option specifying information such as: TFTP server and Avaya Media Server Gatekeeper IP Addresses, or SIP-specific parameters, such as SIPPROXYSRVR, as defined in 4600 Series IP Telephone Customizable System Parameters. Use the Site-Specific Option Number (SSON) at #176. You can set this option value, for example, to either of the following strings:

  MCIPADD=*xxx.xxx.xxx.xxx*,MCPORT=*yyyy*,TFTPDIR=*<path>*,TFTPSRVR=*zzz.zzz.zzz.zzz*

  OR

  MCIPADD=*{list of DNS names}*, MCPORT=*yyyy*, TFTPDIR=*<path>*, TFTPSRVR= *{list of DNS names}*

  As of Release 2.4, also use Option 176 to identify the VLAN IDs used for the Ethernet line interface and the secondary Ethernet interface for VLAN separation. In this instance, if your voice VLAN ID is ***xxx*** and your data VLAN ID is ***yyy***, at a minimum, add the following string to Option 176:

  L2Q=1,L2QVLAN=*xxx*,PHY2VLAN=*yyy*

  The following is the recommended format for VLAN separation on dynamically programmed IP telephones. In this example,

  L2Q=1,L2QVLAN=*xxx*,VLANSEP=1,PHY2VLAN=*yyy*,PHY2PRIO=*z*

  To enable VLAN separation, also set related parameters in the 46xxsettings.txt file, as described in 4600 Series IP Telephone Scripts and Application Files on page 74.

Note:

The total length of the DHCP packet cannot exceed 576 bytes.

List the TFTPDIR value before the TFTPSRVR value, if the latter is specified in the SSON.

Some DHCP applications limit the length of Option 176 to 247 characters.

You can have SIP-specific, H.323-specific, or common system parameters in the same SSON Option. All such parameters are downloaded to all IP telephones, but only the relevant parameters for a given telephone are acted upon.

The 4600 Series IP Telephones do not support Regular Expression Matching, and therefore, do not use wildcards. See Administering Options for the 4600 Series IP Telephones on page 96.

In configurations where the upgrade script and application files are in the default directory, do not use the TFTPDIR=<path>.

You do not have to use Option 176. If you do not use this option, you must ensure that the key information, especially TFTPSRVR, MCIPADD, and MCPORT, is administered appropriately elsewhere. For example, when you specify the DNS server in Option 6, and the Domain Name in Option 15, you can use the configured names “AvayaTFTPServer” and “AvayaCallServer” for TFTPSRVR and MCIPADD, respectively. Upgrading from IP telephone Releases prior to R1.60 requires Option 176 to be minimally administered with MCIPADD.

Administer DHCP servers to deliver only the options specified in this document. Administering additional, unexpected options might have unexpected consequences, including possibly causing the IP telephone to ignore the DHCP server.

The media server name and TFTP server name must each be no more than 32 characters in length.

Note:

Examples of good DNS administration include:

- Option 6: "***aaa.aaa.aaa.aaa***"
- Option 15: "***dnsexample.yourco.com***"
- Option 66: "***tftpserver.yourco.com,zzz.zzz.zzz.zzz***"
- Option 176: "**MCIPADD=*xxx.xxx.xxx.xxx***"

Depending on the DHCP application you choose, be aware that the application most likely will not immediately recycle expired DHCP leases. An expired lease might remain reserved for the original client for a day or more. For example, Windows NT® DHCP reserves expired leases for about one day. This reservation period protects a client's lease for a short time. If the client and the DHCP server are in two different time zones, the computers' clocks are not in synch, or the client is not on the network when the lease expires, there is time to correct the situation.

The following example shows the implication of having a reservation period: Assume two IP Addresses, therefore two possible DHCP leases. Assume three IP telephones, two of which are using the two available IP Addresses. When the lease of the first two telephones expires, the third telephone cannot get a lease until the reservation period expires. Even if you remove the other two telephones from the network, the third telephone remains without a lease until the reservation period expires.

In Table 4, the 4600 Series IP Telephone sets the system values to the DHCPACK message field values shown.

Table 4: DHCPACK Setting of System Values

System Value	Set to
IPADD	The **yiaddr** field.
NETMASK	Option #1 (if received).
GIPADD	The first four octets of Option #3 (if received).
TFTPSRVR	The first four octets of the **siaddr** field.

The rest of this section describes some common DHCP servers.

Windows NT 4.0 DHCP Server

This section contains details on how to verify and configure the DHCP server included in the Windows NT® 4.0 server operating system.

Use Verifying the Installation of the DHCP Server to verify whether the DHCP server is installed. If it is not, install the DHCP server. If it is installed, go to the section Initial Configuration on page 63 and the subsequent sections.

Verifying the Installation of the DHCP Server

Use the following procedure to verify whether the DHCP server is installed.

1. Select **Start**-->**Settings**-->**Control Panel**.
2. Double-click the **Network** icon.
3. Verify that **Microsoft DHCP Server** is listed as one of the Network Services on the Services tab.
4. If it is listed, go to the following section, Initial Configuration. If it is not listed, then install the DHCP server.

Initial Configuration

The Windows NT® 4.0 DHCP server configuration involves setting up a scope for the IP telephone. A DHCP scope is essentially a grouping of IP devices, in this case IP telephones, running the DHCP client service in a subnet. The scope defines parameters for each subnet. Each scope has the following properties:

- A unique subnet mask used to determine the subnet related to a given IP Address.
- A scope name assigned by the administrator when the scope is created.
- Lease duration values to be assigned to DHCP clients with dynamic addresses.

In addition, the DHCP server can assign configuration parameters to a client, and these can be specified for each DHCP scope.

Setting up the Windows NT® 4.0 DHCP server requires the following steps:

1. Creating a DHCP scope for the IP telephones.
2. Editing custom options.
3. Adding the DHCP options.
4. Activating the new scope.
5. Verifying your configuration.

Each step is detailed in the next five sub-sections.

Creating a DHCP Scope for the IP Telephones

Use the following procedure to create a DHCP scope for the IP telephones.

1. Select **Start**-->**Programs**-->**Admin Tools**-->**DHCP Manager**.
2. Expand **Local Machine** in the DHCP Servers window by double clicking it until the **+** sign changes to a **-** sign.
3. Select **Scope**-->**Create**.
4. Define the range of IP Addresses used by the IP telephones listed in Table 3: Required Network Information Before Installation - Per DHCP Server.

   The **Start Address** is the first IP Address to be used for the IP telephones.

   The **End Address** is the last IP Address to be used for the IP telephones.

   Set the **Subnet Mask** to the value recorded in Table 3: Required Network Information Before Installation - Per DHCP Server.

   To ***exclude*** any IP Addresses you do not want assigned to IP telephones within the **Start** and **End** Addresses range:

   a. In the **Exclusion Range Start Address** field, enter the ***first IP Address*** in the range that you want to exclude.

   b. In the **Exclusion Range End Address** field, enter the ***last IP Address*** in the range that you want to exclude.

   c. Click the **Add** button.

   d. Repeat steps a. through c. for each IP Address range to be excluded.

      Example:

      Suppose the range of IP Addresses available for your IP telephone network are:

      - 135.254.76.7 to 135.254.76.80
      - 135.254.76.90 to 135.254.76.200
      - 135.254.76.225 to 135.254.76.230

      Your start address and end address are 135.254.76.7 and 135.254.76.230 respectively.

      Exclude the ranges 135.254.76.81 to 135.254.76.89 and 135.254.76.201 to 135.254.76.224.

   Note:

   We recommend that you provision the 4600 Series IP Telephones with sequential IP Addresses.

   We recommend not mixing 4600 Series IP Telephones and PCs in the same scope.

5. Under **Lease Duration**, select the **Limited To** option and set the ***lease duration*** to the maximum.
6. Enter a ***sensible name*** for the **Name** field, such as “DEFINITY IP Telephones.”
7. Click **OK**.

   A dialog box prompts you: `Activate the new scope now?`
8. Click **No**.

Note:

Activate the scope only after setting all options.

Editing Custom Options

Use the following procedure to edit custom options.

1. Highlight the newly created scope.
2. Select **DHCP Options**-->**Defaults** in the menu.
3. Click the **New** button.
4. In the **Add Option Type** dialog box, enter an appropriate custom option name, for example, “46XXOPTION.”
5. Change the **Data Type Byte** value to **String**.
6. Enter **176** in the **Identifier** field.
7. Click the **OK** button.

   The **DHCP Options** menu displays.
8. Select the **Option Name** for 176 and set the *value string*.
9. Click the **OK** button.
10. For the **Option Name** field, select **003 Router** from the drop-down list.
11. Click **Edit Array**.
12. Enter the ***Gateway IP Address*** recorded in Table 3: Required Network Information Before Installation - Per DHCP Server for the **New IP Address** field.
13. Select **Add** and then **OK**.

Adding the DHCP Option

Use the following procedure to add the DHCP option.

1. Highlight the scope you just created.
2. Select **Scope** under **DHCP Options**.
3. Select the **176 option** that you created from the **Unused Options** list.
4. Click the **Add** button.
5. Select **option 003** from the **Unused Options** list.
6. Click the **Add** button.
7. Click the **OK** button.
8. Select the **Global parameter** under **DHCP Options**.
9. Select the **176 option** that you created from the **Unused Options** list.
10. Click the **Add** button.
11. Click the **OK** button.

Activating the Leases

Use the following procedure to activate the leases.

1. Click **Activate** under the **Scope** menu.

   The light-bulb icon for the scope lights.

Verifying Your Configuration

This section describes how to verify that the **46XXOPTIONs** are correctly configured for the Windows NT® 4.0 DHCP server.

Verify the Default Option, 176 46XXOPTION

Use the following procedure to verify the default option.

1. Select **Start**-->**Programs**-->**Admin Tools**-->**DHCP Manager**.
2. Expand **Local Machine** in the DHCP servers window by double clicking until the **+** sign changes to a **-** sign.
3. In the DHCP servers frame, click the *scope* for the IP telephone.
4. Select **Defaults** from the **DHCP_Options** menu.
5. In the **Option Name** pull-down list, select **176 46XXOPTION**.
6. Verify that the **Value String** box contains the correct string from DHCP Software Alternatives on page 58.

   If not, update the string and click the **OK** button twice.

Verify the Scope Option, 176 46XXOPTION

Use the following procedure to verify the scope option:

1. Select **Scope** under **DHCP OPTIONS**.
2. In the **Active Options:** scroll list, click **176 46XXOPTION**.
3. Click the **Value** button.
4. Verify that the **Value String** box contains the correct string from DHCP Generic Setup on page 59.

   If not, update the string and click the **OK** button.

Verify the Global Option, 176 46XXOPTION

Use the following procedure to verify the global option:

1. Select **Global** under **DHCP OPTIONS**.
2. In the **Active Options:** scroll list, click **176 46XXOPTION**.
3. Click the **Value** button.
4. Verify that the **Value String** box contains the correct value from DHCP Generic Setup on page 59. If not, update the string and click the **OK** button.

Windows 2000 DHCP Server

This section describes the configuration of the DHCP server in Windows 2000®.

Verifying the Installation of the DHCP Server

Use the following procedure to verify whether the DHCP server is installed.

1. Select **Start**-->**Program**-->**Administrative Tools**-->**Computer Management**.
2. Under **Services and Applications** in the Computer Management tree, find **DHCP**.
3. If DHCP is not installed, install the DHCP server. Otherwise, proceed directly to Creating and Configuring a DHCP Scope for instructions on server configuration.

Creating and Configuring a DHCP Scope

Use the following procedure to create and configure a DHCP scope.

1. Select **Start**-->**Programs**-->**Administrative Tools**-->**DHCP**.
2. In the console tree, click the *DHCP server* to which you want to add the DHCP scope for the IP telephones. This is usually the name of your DHCP server machine.
3. Select **Action**-->**New Scope** from the menu.

   Windows displays the **New Scope Wizard** to guide you through rest of the setup.
4. Click the **Next** button.

   The **Scope Name** dialog box displays.
5. In the **Name** field, enter a name for the scope such as “DEFINITY IP Telephones,” then enter a brief comment in the **Description** field.
6. When you finish Steps 1 - 5, click the **Next** button.

   The **IP Address Range** dialog box displays.
7. Define the range of IP Addresses used by the IP telephones listed in Table 3: Required Network Information Before Installation - Per DHCP Server. The **Start IP Address** is the first IP Address available to the IP telephones. The **End IP Address** is the last IP Address available to the IP telephones.

   Note:

   We recommend not mixing 4600 Series IP Telephones and PCs in the same scope.
8. Define the **subnet mask** in one of two ways:
   - The number of bits of an IP Address to use for the network/subnet IDs.
   - The subnet mask IP Address.

   Enter only one of these values. When you finish, click the **Next** button. The **Add Exclusions** dialog box displays.
9. Exclude any IP Addresses in the range specified in the previous step that you do not want assigned to an IP telephone.
   a. In the **Start Address** field under **Exclusion Range**, enter the ***first IP Address*** in the range you want to exclude.
   b. In the **End Address** field under **Exclusion Range**, enter the ***last IP Address*** in the range you want to exclude.
   c. Click the **Add** button.
   d. Repeat steps a. through c. for each IP Address range that you want to exclude.

Note:

You can add additional exclusion ranges later by right clicking the **Address Pool** under the newly created scope and selecting the **New Exclusion Range** option.

Example:

Suppose the ranges of IP Addresses available for your IP telephone network are:

- 135.254.76.7 to 135.254.76.80
- 135.254.76.90 to 135.254.76.200
- 135.254.76.225 to 135.254.76.230

The Start IP Address and End IP Address you enter in the **IP Address Range** dialog box are 135.254.76.7 and 135.254.76.230 respectively.

In the Add Exclusions dialog box, exclude the following ranges:

- 135.254.76.81 to 135.254.76.89
- 135.254.76.201 to 135.254.76.224

Click the **Next** button after you enter all the exclusions.
The **Lease Duration** dialog box displays.

10. For all telephones that obtain their IP Addresses from the server, enter **30 days** in the **Lease Duration** field. This is the duration after which a device's IP Address expires and which the device needs to renew.
11. Click the **Next** button.

    The **Configure DHCP Options** dialog box displays.
12. Click the **No, I will activate this scope later** button.

    The **Router** (Default Gateway) dialog box displays.
13. For each router or default gateway, enter the ***IP Address*** and click the **Add** button.

    When you are done, click the **Next** button.
    The **Completing the New Scope Wizard** dialog box displays.
14. Click the **Finish** button.

    The new scope appears under your server in the DHCP tree. The scope is not yet active and will not assign IP Addresses.
15. Highlight the newly created scope and select **Action**-->**Properties** from the menu.
16. Under **Lease duration for DHCP clients**, select **2 weeks** (minimum) and click the **OK** button.

CAUTION:

IP Address leases are kept active for varying periods of time. To avoid having calls terminated suddenly, ensure that the lease duration is not too short, for example, not set to less than two weeks. A lease duration of two to four weeks is reasonable.

Adding DHCP Options

Use the following procedure to add DHCP options to the scope you created in the previous procedure.

1. On the DHCP window, right-click the **Scope Options** folder under the scope you created in the last procedure.

   A drop-down menu displays.

2. Click the **Configure Options...** option.

   The **Scope Options** dialog box displays.

3. In the General tab page, under the **Available Options**, check the **066'Boot Server Host Name' Options** checkbox.

   The **String Value** dialog box displays.

4. Enter the ***TFTP Server address(es)*** in the **String Value**. Use the same TFTPSRVR value format as discussed in TFTP Generic Setup on page 72. For example, if you had a TFTP server at IP Address "*zzz.zzz.zzz.zzz*" and a second TFTP server at address "tftpserver.yourco.com," in the string value enter:

   "zzz.zzz.zzz.zzz,tftpserver.yourco.com"

5. In the left pane of the DHCP, right click the **DHCP Server name**, then click **Set Predefined Options...**.

6. Under **Predefined Options and Values**, click **Add**.

7. In the **Option Type Name** field, enter ***any appropriate name***, for example, "Avaya IP Telephones."

8. Change the **Data Type** to **String**.

9. In the **Code** field, enter **176**, then click the **OK** button twice.

   The **Predefined Options and Values** dialog box closes, leaving the DHCP dialog box enabled.

10. Expand the newly created scope to reveal its **Scope Options**.

11. Click **Scope Options** and select **Action**-->**Configure Options** from the menu.

12. In the **General** tab page, under the **Available Options**, check the **Option 176** checkbox.

13. In the **Data Entry** box, enter the ***DHCP IP telephone option string*** as described in DHCP Generic Setup on page 59.

    Note:

    You can enter the text string directly on the right side of the **Data Entry** box under the ASCII label.

14. From the list in **Available Options**, check option **003 Router**.
15. Enter the ***gateway (router) IP Address*** from the IP Address field of Table 3: Required Network Information Before Installation - Per DHCP Server.
16. Click the **Add** button.
17. Click the **OK** button.

Activating the New Scope

Use the following procedure to activate the new scope.

1. In the DHCP console tree, click the **IP Telephone Scope** you just created.
2. From the **Action** menu, select **Activate**.

   The small red down arrow over the scope icon disappears, indicating that the scope was activated.

TFTP (H.323 Only)

This section describes how to set up a TFTP server for downloading software updates to the 4600 Series IP Telephones.

CAUTION:

The files defined by the TFTP server configuration have to be accessible from all IP telephones. Ensure that the filenames match the names in the upgrade script, including case, since UNIX systems are case-sensitive.

Note:

SIP IP telephones download upgrade script files, and hence, firmware and settings files, from HTTP servers only.

You can use any TFTP application you want. However, Avaya recommends using the TFTP server capability on the S8300 media server or the Avaya IP Telephone File Server Application.

TFTP Generic Setup

The following phases are involved in setting up a TFTP server.

- Install the TFTP server software.
- Configure the file path parameter to the directory where the files are to be stored. This is the file path in Table 3: Required Network Information Before Installation - Per DHCP Server on page 57. For increased security, we also recommend that you disable the ability to upload to the server. Note that this option might not be available to all TFTP servers.
- Download the upgrade script file and application file from the Avaya Web site (http://www.avaya.com/support) to the directory as specified by the file path.
- Table 10, Table 11, and Table 12 list the parameters you can administer when manually creating the TFTP script file. Manual administration is discussed in 4600 Series IP Telephone Scripts and Application Files.

  Note:

  Many LINUX servers distinguish between uppercase and lowercase names. Ensure that you accurately specify the 46xxsettings filename, and the names and values of the data therein.

TFTP Server on S8300 Media Server

The S8300 Media Server provides all the TFTP support required for the 4600 Series IP Telephones. In addition, the media server has an easy to use, PC-based interface for creating script files. Thus, you do not need to manually create the text files discussed in 4600 Series IP Telephone Scripts and Application Files. The media server creates the files for you. For more information about the media server, see *Downloading Avaya 46xx IP Telephone Software Using Avaya Media Servers*, mentioned in Related Documents.

Avaya File Server Application

The Avaya IP Telephone File Server Application provides a Windows or Linux TFTP or HTTP Server you can install on your own server. For more information, see *Avaya IP Telephone File Server Application Reference Guide* (Document # 16-601433), mentioned in Related Documents and available from the Avaya support Web site.

HTTP

This section gives general guidance to set up an HTTP server for downloading software updates to 4600 Series IP Telephones.

CAUTION:

The files defined by HTTP server configuration must be accessible from all IP telephones invoking those files. Ensure that the file names match the names in the upgrade script, including case, since UNIX systems are case-sensitive.

Note:

Use any HTTP application you want. In addition to the HTTP application on the Avaya S8300 Media Server, other commonly used HTTP applications include Apache and Microsoft IIS.

HTTP and HTTPS does not apply to the 4690 IP Telephone.

HTTP Generic Setup

These are the phases involved in setting up an HTTP server:

- Install the HTTP server application.
- Administer the system parameter HTTPSRVR to the address(es) of the HTTP server. Include this parameter in DHCP Option 176, or the appropriate SSON Option.
- Download the upgrade script file and application file(s) from the Avaya Web site http://www.avaya.com/support to the HTTP server.

  Note:

  Many LINUX servers distinguish between upper and lower case names. Ensure that you specify the 46xxsettings filename accurately, as well as the names and values of the data within the file.

If you choose to enhance the security of your HTTP environment by using Transport Layer Security (TLS), you also need to:

- Install the TLS server application.
- Administer the system parameter TLSSRVR to the address(es) of the Avaya HTTP server.

  Note:

  TLS is supported only on an Avaya server.

4600 Series IP Telephone Scripts and Application Files

Important:

You can convert a 4602, 4602SW, 4602SW+, 4610SW, 4620SW, 4621SW, and 4625SW IP Telephone from H.323 to SIP software, or from SIP to H.323 software. However, depending on the telephone model and the software version you start from, additional steps may be required from those mentioned in this section. When converting from one protocol type to another on a given telephone, please see “Converting Software on Avaya 4600 Series IP Telephones” in the *4600 Series IP Telephone Installation Guide* (Document Number 555-233-128).

The files necessary to operate the 4600 Series IP Telephones are available on the Avaya Web site at: http://www.avaya.com/support.

Two files on the file server are essential. Other files are needed when the Avaya IP Telephones need an upgrade. The essential files are:

- An upgrade script file, which tells the IP telephone whether the telephone needs to upgrade software. The Avaya IP Telephones attempt to read this file whenever they reset. The upgrade script file is also used to point to the settings file. There are separate upgrade script files for the 4630 Telephones.

  Note:

  The 4630 IP Telephones have a different upgrade process than the other telephones. This is because the 4630 touch screen operation is significantly more complex than any of the other Avaya IP Telephones. There are some common elements between the 4630 and other IP telephones. Any differences are highlighted as appropriate in this section.

- The settings file contains the option settings that enable many of the options you will need to customize the Avaya IP Telephones for your enterprise. You can use one settings file for all your Avaya IP Telephones.

In addition to the upgrade script and settings files you need the latest binary code used in the Avaya IP Telephones.

The upgrade script file and settings file are available from the Avaya Web site. The files allow you to upgrade to new software releases and new functionality without having to replace IP telephones. These two files, plus other useful information such as a ReadMe file, information about infrared capabilities, and a settings file template, are contained in a self-extracting executable file you download to your file server. Application files for all current 4600 Series IP Telephones except the 4630/4630SW, and an upgrade script file, are bundled together in that self-extracting executable file. The self-extracting executable file comes in both zipped and unzipped format. See Choosing the Right Application File and Upgrade Script File on page 76 for more information.

The Avaya-provided upgrade script files, and the binaries included in the zip files, upgrade the Avaya IP Telephones. You should not need to modify them. It is essential that all the binary files be together on the file server. When downloading a new release onto a file server with an existing release already on it, we recommend that you:

- Stop the file server.
- Back up all the current file server directories as applicable.
- Copy your ***46xxsettings.txt*** file to a backup location.
- Remove all the files in the download directory. This ensures that you do not have an inappropriate binary or configuration file on the server.
- Download the self-extracting executable file, or the corresponding zip file.
- Extract all the files. When extracting the 4630 files, ensure that you allow the directories to be created.
- Copy your ***46xxsettings.txt*** file back into the download directory.
- Check the Readme files for release-specific information.
- Modify the ***46xxsettings.txt*** file as desired.
- Restart the TFTP/HTTP Server.
- Reset your Avaya IP Telephones.

You can download a default upgrade script file, sometimes called merely the “script file,” from http://www.avaya.com/support. This file allows the telephone to use default settings for customer-definable options. Of course, these settings can also be changed with DHCP or in some cases, from the telephone’s dialpad itself. However, you might want to open the default file and administer the options to add useful functionality to your Avaya IP Telephones. This file must reside in the same directory as the upgrade script file, and must be called ***46xxsettings.scr*** or ***46xxsettings.txt***. The Avaya IP Telephones can operate without this file.

Note:

Most Windows systems interpret the file extension ***.scr** as a screen saver. The 4600 IP Telephones originally used *.scr to indicate a script file. Starting with Release 1.7, the settings file can also have the extension ***.txt**.

The settings file can include any of the five types of statements, one per line:

- Comments, which are statements with a “#” character in the first column.
- Tags, which are comments that have exactly one space character after the initial #, followed by a text string with no spaces.
- `Goto` commands, of the form **GOTO *tag.*** `Goto` commands cause the telephone to continue interpreting the settings file at the next line after a **# *tag*** statement. If no such statement exists, the rest of the settings file is ignored.
- Conditionals, of the form **IF *$name* SEQ *string* GOTO *tag***. Conditionals cause the `Goto` command to be processed if the value of ***name*** is a case-insensitive equivalent to ***string***. If no such ***name*** exists, the entire conditional is ignored.
- `SET` commands, of the form **SET *parameter_name value***. Invalid values cause the specified value to be ignored for the associated ***parameter_name*** so the default or previously administered value is retained. All values must be text strings, even if the value itself is numeric, a dotted decimal IP Address, etc.

Note:

Enclose all data in quotation marks for proper interpretation.

The Avaya-provided upgrade script file includes lines that tell the telephone to **GET *46xxsettings.scr*** and ***46xxsettings.txt***. These lines cause the telephone to use TFTP/HTTP to attempt to download the file specified in the **GET** command. If the file is obtained, its contents are interpreted as an additional script file. That is how your settings are changed from the default settings. If the file cannot be obtained, the telephone continues processing the upgrade script file. The upgrade script file is processed so that if there is no 46xxsettings.scr file, the telephone looks for a 46xxsettings.txt file. If the settings file is successfully obtained but does not include any setting changes the telephone stops using TFTP or HTTP. This happens when you initially download the script file template from the Avaya support Web site, before you make any changes. When the settings file contains no setting changes, the telephone does not go back to the upgrade script file.

You can change the settings file name, if desired, as long as you also edit the corresponding **GET** command in the upgrade script file. However, we encourage you **not** to alter the Avaya-provided upgrade script file. If Avaya changes the upgrade script file in the future, any changes you have made will be lost. We strongly encourage you to use the ***46xxsettings*** file to customize your settings instead.

For more details on customizing your settings file, see Contents of the Settings File.

Choosing the Right Application File and Upgrade Script File

The 4600 IP Telephone software Releases are bundled together in ****exe*** and ****zip*** files on the Avaya support Web site. See 4600 Series IP Telephone Scripts and Application Files for a detailed description. As of Release 2.7, you have four “bundles” from which to choose. Only one bundle is likely to be optimal for any one environment.

Which bundle to choose depends on the answer to two questions:

- Which version of 4610SW/4620SW software do you need in that environment?
- Are the majority of your 4602/4602SW/4602SW+, 4610SW, 4620SW, 4621SW, and 4625SW Telephones in that environment H.323-based or SIP-based?

The 4610SW, 4620SW, 4621SW, 4622SW, and 4625SW IP Telephones support multi-byte characters, so the software bundles come in one of four versions:

- a default version which only supports single-byte characters like those used in English, French, Japanese Katakana, etc.
- a multi-byte version for 4610SW, 4620SW, 4621SW, 4622SW, and 4625SW IP Telephones that support Chinese, Russian, and Hebrew.
- a separate multi-byte version for 4610SW, 4620SW, 4621SW, 4622SW and 4625SW IP Telephones that support Japanese, Russian, and Hebrew. Note that the 4625SW does not currently support Japanese (Kanji).
- a separate multi-byte version for 4610SW, 4620SW, 4621SW, 4622SW and 4625SW IP Telephones that support Korean, Russian, and Hebrew.

If multi-byte support is not relevant to you, select the default bundle, even if you do not have any 4610SW, 4620SW, 4621SW, 4622SW, and 4625SW telephones. Otherwise, select the software bundle that includes Chinese, Japanese, or Korean as appropriate.

Note:

All bundles include the complete software for the other, non-4610SW/4620SW/4621SW/4622SW/4625SW Telephones. The software includes the 4620 IP Telephone, but not the 4630/4630SW, which remains separate. The only differences between the four bundles are the software for the 4610SW, 4620SW, 4621SW, 4622SW, and 4625SW, and a slight change in the associated upgrade script file.

The 4602/4602SW/4602SW+, 4610SW, 4620SW, 4621SW and 4625SW IP Telephones can support either H.323 or SIP signaling protocols. If a majority of your 4600 Series IP Telephones are H.323-based, which is the most common situation, you can use any or all of the software bundles identified in this section. If a majority are SIP-based, select the fourth software bundle, identified as the “SIP” software bundle on the Web site. The application files in this SIP software bundle are the same as in the default bundle. The difference is a modified upgrade script file that assumes SIP is the default protocol for 4602/4602SW/4602SW+, 4610SW, 4620SW, 4621SW, and 4625SW IP Telephones, and that H.323 is the exception.

When you have a mixture of H.323 and SIP telephones, use the **SIG** system value to ensure that each telephone type has appropriate software downloaded. The **SIG** system value has three legal values:

- the default value “**0**” which indicates “use the default protocol,”
- “**1**” meaning “use H.323,” and
- “**2**” meaning “use SIP.”

You decide the meaning of “the default protocol.” If the majority of your IP telephones are H.323-based, that should be the default. Otherwise, SIP is the default.

The SIG system value cannot be set in the 46xxsettings file or in the upgrade script file. SIG can only be set on a telephone-by-telephone basis. Instead of manually setting SIG yourself, first instruct the installers of the non-default phones to perform the SIGnaling Protocol Identifier procedure in Chapter 3 of the *4600 Series IP Telephone Installation Guide*. For example, if yours is a largely H.323 environment, when SIP phones are installed the SIG system value should be set to “**2**.” If yours is a largely SIP environment, when H.323 phones are installed the SIG system value should be set to “**1**.”

Detailed information about SIP is available in the SIP-related documentation, provided elsewhere on the Avaya support Web site.

Note:

As indicated above, although the SIG system value is a Release 2.0 feature, the 4601 IP Telephone supports SIG functionality, even though the 4601 currently supports only Release 1.8 software.

Contents of the Upgrade Script

See Appendix F: Sample Upgrade Script File for a typical upgrade script file.

Contents of the Settings File

Check the last lines of the Upgrade Script file example in the previous section. They show that after checking the application software, the 4600 Series IP Telephone looks for a 46xx settings file. This optional file is under your control and is where you can identify non-default option settings, application-specific parameters, etc. The Avaya support Web site has a template for this file for downloading. An example of what the file could look like follows.

Note:

The following is intended only as an example. Your settings will vary from the settings shown. This sample assumes specification of a DNS Server, parameters for the 4630/4630SW Directory application, and a 4620 Web Browser. See Administering Options for the 4600 Series IP Telephones on page 96, for details about specific values. You need only specify settings that vary from defaults, although specifying defaults is harmless.

```
DNSSRVR=”dnsexample.yourco.com”

DIRSRVR=”123.123.123.123”
DIRTOPDN=”yourco”

WMLHOME=”http://support.avaya.com/elmodocs2/avayaip/4620/home.wml”
WEBPROXY=”11.11.11.11”
```

As of Release 2.4, VLAN separation provides for tagged frames to be received by a secondary Ethernet interface, typically a PC. Add commands to the 46xxsettings.txt file to enable VLAN separation, provide the VLAN ID for tagged frames received on the secondary Ethernet interface, and set the Layer 2 priority for those tagged frames. The following example assumes the data VLAN ID is “yyy” and the data traffic priority is “z”:

```
SET VLANSEP 1
SET PHY2VLAN yyy
SET PHY2PRIO z
```

The GROUP System Value

You might have different communities of end users, all of which have the same model telephone, but which require different administered settings. For example, you might want to restrict Call Center agents from being able to Logoff, which might be an essential capability for "hot-desking" associates. Or you might want to assign your SIP telephone users to different messaging systems or registration/proxy servers. We provide examples of the group settings for each of these situations later in this section.

As of Release 2.0, the simplest way to separate groups of users is to associate each of them with a number. You then edit the 46xxsettings file so each group is assigned the appropriate settings. Use the GROUP system value for this purpose. The GROUP system value **cannot** be set in the 46xxsettings file. The GROUP System value can only be set on a telephone-by-telephone basis. To do so, first identify which phones are associated with which group, and designate a number for each group. The number can be any integer from 0 to 999, with 0 as the default, meaning your largest group would be assigned as Group 0.

Then, at each non-default telephone, instruct the installer or end-user to invoke the GROUP Local (dialpad) Administrative procedure as specified in the *4600 Series IP Telephone Installation Guide* and specify which GROUP number to use. Once the GROUP assignments are in place, edit the settings file to allow each telephone of the appropriate group to download its proper settings.

Here is an example of the settings file for the Call Center agent:

```
IF $GROUP SEQ 1 goto CALLCENTER
IF $GROUP SEQ 2 goto HOTDESK
{specify settings unique to Group 0}
goto END

# CALLCENTER
{specify settings unique to Group 1}
goto END

# HOTDESK
{specify settings unique to Group 2}

# END
{specify settings common to all Groups}
```

Here is an example of the settings file for the SIP telephone users. Note that there are two messaging systems and two registration/proxy servers, for a total of four possible combinations. These sample GROUP assignments are unique to the SIP users. Other GROUP assignments could be in the same file for other purposes.

```
IF $GROUP SEQ 10 goto GROUP10
IF $GROUP SEQ 20 goto GROUP20
IF $GROUP SEQ 30 goto GROUP30
IF $GROUP SEQ 40 goto GROUP40
```

```
{specify settings unique to Group 0}
goto END

# GROUP10
{specify settings unique to Group 10, for example}
SET COVERAGEADDR "22000"
SET SIPPROXYSRVR "{IP Address of server1}"
SET SIPREGISTRAR "{IP Address of server1}"
goto END

# GROUP20
{specify settings unique to Group 20, for example}
SET COVERAGEADDR "23000"
SET SIPPROXYSRVR "{IP Address of server1}"
SET SIPREGISTRAR "{IP Address of server1}"
goto END

# GROUP30
{specify settings unique to Group 30, for example}
SET COVERAGEADDR "22000"
SET SIPPROXYSRVR "{IP Address of server2}"
SET SIPREGISTRAR "{IP Address of server2}"
goto END

# GROUP40
{specify settings unique to Group 40, for example}
SET COVERAGEADDR "23000"
SET SIPPROXYSRVR "{IP Address of server2}"
SET SIPREGISTRAR "{IP Address of server2}"
goto END

# END
{specify settings common to all Groups}
```

QoS

The 4600 Series IP Telephones support both IEEE 802.1D/Q and DiffServ. Other network-based QoS initiatives such as UDP port selection do not require support by the telephones. Those initiatives nonetheless can contribute to improved QoS for the entire network.

IEEE 802.1D and 802.1Q

IEEE's 802.1Q standard defines a tag that can be added to voice and data packets. Most of the information associated with this tag deals with Virtual LAN (VLAN) management, but 3 bits are reserved for identifying packet priority. These 3 bits allow any one of 8 priorities to be assigned to a specific packet. As defined in the standard, the 8 priorities are, from highest to lowest:

- 7: Network management traffic
- 6: Voice traffic with less than 10ms latency
- 5: Voice traffic with less than 100ms latency
- 4: "Controlled-load" traffic for mission-critical data applications
- 3: Traffic meriting "extra-effort" by the network for prompt delivery, for example, executives' e-mail
- 2: Reserved for future use
- 0: Traffic meriting the network's "best-effort" for prompt delivery. This is the default priority.
- 1: Background traffic such as bulk data transfers and backups

Note:

Priority 0 is a higher priority than Priority 1.

To support IEEE 802.1D/Q, the 4600 Series IP Telephones can be administered either of two ways:

- from the network by appropriate administration of the DHCP or TFTP/HTTP servers, as covered in 4600 Series IP Telephone Scripts and Application Files on page 74, or
- at the telephone itself using dialpad input, as covered under local administrative procedures in the *4600 Series IP Telephone Installation Guide*.

Eight IEEE 802.1D/Q QoS parameters in the telephones can be administered, as follows. The first five parameters are for standard 802.1Q tagging and apply to any 4600 Series IP Telephone. The last three parameters apply to all 4600 Series IP Telephones with a secondary Ethernet interface.

- **L2Q:** 802.1Q framing parameter (1=On, 2=Off, or 0=AUTO). The default is 0, but the preferred setting is 1 (ON). You can manually set the L2Q value of a specific 4600 IP Telephone to any value, for example, AUTO, ON, or OFF. However, any subsequent value administered via DHCP or TFTP/HTTP settings file will override the manual value. To use the **QoS** Local Administrative Option to set L2Q manually see the *4600 Series IP Telephone Installation Guide.*
- **L2QVLAN:** the VLAN ID on which the telephone should operate. For example, what VLAN ID to use for DHCP Discovery, etc. (up to 4 digits, from 0 to 4094, default is 0).
- **VLANTEST:** the number of seconds to wait for a DHCPOFFER when using a non--zero VLAN ID (up to 3 digits, from 0 to 999, default is 60).

- **L2QAUD:** 802.1Q VoIP (voice) user RTP traffic priority value (between 0 and 7, default is 6).
- **L2QSIG:** 802.1Q VoIP (voice) user Call Control Signaling traffic priority value (between 0 and 7, default is 6).
- **VLANSEP:** enables VLAN separation when set to 1 (the default); disables VLAN separation when set to 0. If the value is zero, broadcasts are transmitted. Can only be administered using DHCP/TFTP, not by a manual procedure.
- **PHY2VLAN:** VLAN ID to be used for tagged (data) frames received on the secondary Ethernet interface when VLAN separation is enabled (up to 4 digits, from 0 to 4094, default is 0). Can only be administered using DHCP/TFTP, not by a manual procedure.
- **PHY2PRIO:** Layer 2 (data) priority value to be used for tagged frames received on the secondary Ethernet interface when VLAN separation is enabled (1 digit, 0 (zero) through 7, default is 0). Can only be administered using DHCP/TFTP, not by a manual procedure.

In the *4600 Series IP Telephone Installation Guide*, the Local Administrative Option ADDR also allows you to specify VLAN IDs and VLANTEST values. The Local Administrative Option QoS allows you to specify values for L2Q, L2QAUD, and L2QSIG.

The 4600 Series IP Telephones can simultaneously support receipt of packets using, or not using, 802.1Q parameters.

For additional information on VLAN administration, see VLAN Considerations on page 86.

DIFFSERV

IETF RFCs 2474 and 2475 define “services” basically as different ways to treat a network’s different traffic subsets at the Internet Protocol (IP) layer, Layer 3. For example, some packets might be routed to expedite delivery and minimize delay, with other packets routed to minimize loss or cost. Redefining an octet in the Layer 3 headers for IP versions 4, or IPv4 and 6, or IPv6 provides the differentiation between these services (Differentiated Services). IPv4 calls this octet a Type of Service (TOS) octet while IPv6 calls this octet a Traffic Class. In both cases, the octet is interpreted differently than it was originally defined. With Differentiated Services, bits 0 through 5 of the octet identify a Differentiated Services Code Point (DSCP). The DSCP identifies a procedure to be used to handle that packet on a per-hop basis. Bits 6 and 7 of the octet are currently unused, and DSCP-compliant routers ignore them.

With DiffServ, the default DSCP is all zeroes, and represents “no special handling.” RFC 2474 also defines eight “Class Selector Codepoints,” which are the eight DSCP encodings that can be represented by ***xxx*000,** where “***x***” represents one bit. These Code Selector Codepoints are considered prioritized, with the larger numeric values having a higher relative order. DSCP-compliant routers should give the associated packets of larger-valued DSCPs a “probability of timely forwarding” greater than a packet with a lower-valued DSCP. In addition to the eight Class Selector Codepoints, a network can define its own DSCPs by defining

encodings that do not terminate in 000. The specific treatment intended by these custom DSCPs will not necessarily be carried out by routers outside the customer's own network.

The *4600 Series IP Telephone Installation Guide* describes the Local Administrative Option for QoS. This option allows you to specify Diffserv values for Layer 3 audio ("L3QAUD") and signaling traffic ("L3QSIG") on a telephone-by-telephone basis.

The Avaya H.323 IP Telephones' DiffServ values change to the values administered on the media server as soon as the telephone registers. For more information, see the document titled *Administration for Network Connectivity* (555-233-504). Unless there is a specific need in your enterprise LAN, we do not recommend you change the default values.

UDP Port Selection (H.323 Only)

Some data networks include equipment that can perform UDP port selection. This is a mechanism that gives packets with port numbers in a given range priority over packets with port numbers outside that range.

To support UDP port selection, the 4600 Series IP Telephones can be administered from the Avaya Communication Manager Network Region form. Locate specific implementation details for local administration of MCPORT in the *4600 Series IP Telephone Installation Guide*. For Avaya Communication Manager administration, find implementation details in *Administration for Network Connectivity for Avaya Communication Manager Software*. In summary, the system value MCPORT represents the port on the TN2302AP circuit pack. Use this port number to administer routers, etc. supporting UDP port selection, to maximize priority of voice packets being exchanged between the PBX and the telephone.

The default value for **MCPORT** is 1719. Administer the switch to use a port within the proper range for the specific LAN, and the IP telephone(s) will copy that port. A related parameter is **PORTAUD**, which is the RTP port used by the switch. If no UDP port range is administered on the switch, the IP telephone uses an even-numbered port, randomly selected from the interval 4000 to 10000.

Network Audio Quality Display on 4600 Series IP Telephones

With the exceptions of the 4601, 4601+, 4606, 4612, 4624, and 4690 IP Telephones, all Series 4600 IP Telephones are by default administered to allow the end user an opportunity to monitor network audio performance while on a call. The user guides for each telephone provide specific detail on getting to the appropriate screen, what the end user sees, and what the information means.

For 4610SW/4620/4620SW/4621SW/4622SW/4625SW/4630/4630SW IP Telephones, these parameters display in real-time to users on the appropriate screens, while on a call:

Table 5: Parameters in Real-Time

Parameter	Possible Values
Audio Connection Present?	***Yes*** if a receive RTP stream was established. ***No*** if a receive RTP stream was **not** established.
Received Audio Coding	***G.711***, ***G.726A***, or ***G.729***.
Silence Suppression	***Yes*** if the telephone knows the far-end has silence suppression Enabled. ***No*** if the telephone knows the far-end has silence suppression Disabled, or the telephone does not know either way.
Packet Loss	No data or a decimal percentage. Late and out-of-sequence packets are counted as lost if they are discarded. Packets are not counted as lost until a subsequent packet is received and the loss confirmed by the RTP sequence number.
Packetization Delay	No data or an integer number of milliseconds. The number reflects the amount of delay in received audio packets, and includes any look-ahead delay associated with the codec.
One-way Network Delay	No data or an integer number of milliseconds. The number is one-half the value RTCP computes for the round-trip delay.
Network Jitter Compensation Delay	No data or an integer number of milliseconds reporting the average delay introduced by the telephone's jitter buffer.

For 4602/4602SW/4602SW+ IP Telephones, the Network Audio Quality Screen gives the user a qualitative assessment of the current overall audio quality. This assessment is based on separate evaluations of:

- the Packet Loss, and
- the total Network Delay, which is the sum of Packetization Delay, One-way Network Delay, and Network Jitter Compensation Delay, and
- consideration of the codec in use.

This information's implication for LAN administration depends, of course, on the values the user reports and the specific nature of your LAN, like topology, loading, QoS administration, etc. This information's major use is to give the user an idea of how network conditions affect the current call's audio quality. It is assumed you have more detailed tools available for troubleshooting the LAN.

RSVP and RTCP

Avaya IP Telephones implement the Resource ReSerVation Protocol (RSVP) to support WAN bandwidth management. RSVP is administered from the media server. Avaya IP Telephones implement the RTP Control Protocol (RTCP) so Avaya's Voice over IP (VoIP) Monitoring Manager (VMON) software can provide real-time monitoring and historical data of audio quality for VoIP calls.

Resource ReSerVation Protocol (RSVP) is an IETF-standard protocol hosts use to request resource reservations throughout a network. RSVP-compliant hosts send messages through a network to receivers. Receivers respond with messages requesting a type of service and an amount of resources, for example, bandwidth, to carry out that service. The host is responsible for *admitting* (approving) or *rejecting* (denying) the request. In a QoS context, RSVP tries to reserve bandwidth on the network for voice calls on a call-by-call basis. If insufficient bandwidth is available for the target voice quality, a request to use network bandwidth for a voice call is rejected.

RTP Control Protocol (RTCP), as its name implies, is a protocol that provides control functions for Real-time Transport Protocol (RTP). RTP provides end-to-end network services for real-time data such as Voice over IP. But RTP does not provide a reservation function, nor does it guarantee any level of QoS. RTCP supplements RTP by monitoring the quality of the RTP services and can provide real-time information to users of an RTP service. In a QoS context, RTCP is valuable to identify information such as:

- packet loss,
- 1-way delay or how long a packet has to go from source A to destination B,
- jitter, etc.

RTCP itself does not improve QoS, but provides information to help identify where problem areas might be.

You cannot change the telephone's RSVP or RTCP parameters directly on the telephone or by TFTP or DHCP administration. The only way to change these parameters is on the H.323 telephones, and such a change requires appropriate switch administration. See your Avaya Media Server administration documentation for more detail. You cannot change these parameters on a SIP IP telephone.

Internal Audio Parameters

The AUDIOENV variable provides control of some internal audio parameters in the 4600 Series IP Telephones. Avaya does not recommend that customers set these values. In certain situations, particularly in noisy environments, Avaya Tier 4 engineers might recommend that you set the system parameter AUDIOENV.

AUDIOENV is an index into a table that impacts four internal variables:

Table 6: Internal Audio Variables

Variable	Description	Possible Values
AGC_Dyn_Range	AGC dynamic range.	0 for a typical office environment (+/-9dB), 1 for +/-12dB, 2 for +/-15dB, and 3 for +/-18 AGC Dynamic range variation.
Exp_thresh_Hd	The expansion threshold for the headset.	The expansion threshold for the headset has a default value of 0 for a typical office environment, 1 for call center applications, and 2 for “other” audio environments.
Exp_thresh_Hs	The expansion threshold for the handset.	The expansion threshold for the handset has a default value of 0 for a typical office environment, 1 for call center applications, and 2 for “other” audio environments.
Tx_Gain	Transmit gain.	Transmit gain has a default value of 0 for normal transmit gain, 1 for +6dB of gain, and 2 for -6dB of gain.

AUDIOENV is calculated as:

AUDIOENV= (27 * AGC_Dyn_Range) + (9 * Exp_thresh_Hd) + (3 * Exp_thresh_Hs) + Tx_Gain, which results in a range of 0 to 107.

Set AUDIOENV **0** is the nominal setting (**0**,0,0,0)

VLAN Considerations

This section contains information on how to administer 4600 Series IP Telephones to minimize registration time and maximize performance in a Virtual LAN (VLAN) environment. If your LAN environment does not include VLANs, set the system parameter L2Q to 2 (off) to ensure correct operation.

VLAN Tagging

IEEE 802.1Q tagging (VLAN) is a useful method of managing VoIP traffic in your LAN. Avaya recommends that you establish a *voice* VLAN, set L2QVLAN to that VLAN and provide voice traffic with priority over other traffic. If LLDP was used set the telephones’ VLAN, that setting has absolute authority. Otherwise, you can set VLAN tagging manually, by DHCP, or in the 46xxsettings.txt file.

If VLAN tagging is enabled (L2Q= 0 or 1), the 4600 Series IP Telephones set the VLAN ID to L2QVLAN, and VLAN priority for packets from the telephone to L2QAUD for audio packets and L2QSIG for signalling packets. The default value (6) for these parameters is the recommended value for voice traffic in IEEE 802.1D.

Regardless of the tagging setting, a 4600 Series IP Telephone will always transmit packets from the telephone at absolute priority over packets from secondary Ethernet. The priority settings are useful only if the downstream equipment is administered to give the *voice* VLAN priority.

VLAN Detection

The Avaya IP Telephones support automatic detection of the condition where the L2QVLAN setting is incorrect. When VLAN tagging is enabled (L2Q= 0 or 1) initially the 4600 Series IP Telephone transmits DHCP messages with IEEE 802.1Q tagging and the VLAN set to L2QVLAN. The telephones will continue to do this for VLANTEST seconds.

- If the VLANTEST timer expires and L2Q=1, the telephone sets L2QVLAN=0 and transmits DHCP messages with the default VLAN (0).
- If the VLANTEST timer expires and L2Q=0, the telephone sets L2QVLAN=0 and transmits DHCP messages without tagging.
- If VLANTEST is 0, the timer will never expire.

Note:

Regardless of the setting of L2Q, VLANTEST, or L2QVLAN, you must have DHCP administered so that the telephone will get a response to a DHCPDISCOVER when it makes that request on the default (0) VLAN.

After VLANTEST expires, if an Avaya IP Telephone running R2.6 receives a non-zero L2QVLAN value, the telephone will release the IP Address and send DHCPDISCOVER on that VLAN. Any other release will require a manual reset before the telephone will attempt to use a VLAN on which VLANTEST has expired. See the Reset procedure in Chapter 3 of the *4600 Series IP Telephone Installation Guide*.

The telephone ignores any VLAN ID administered on the media server if a non-zero VLAN ID is administered either:

- by LLDP
- manually,
- through DHCP, and/or
- through TFTP or HTTP.

VLAN Separation

In Releases 2.4 and 2.6+, VLAN separation is available to control priority tagging from the device on the secondary Ethernet, typically PC data. The following system parameters control VLAN separation:

- **VLANSEP** - enables (1) or disables (0) VLAN separation.
- **PHY2VLAN** - provides the VLAN ID for tagged frames received on the secondary Ethernet interface.
- **PHY2PRIO** - the layer 2 priority value to be used for tagged frames received on the secondary Ethernet interface.

Table 7 provides several VLAN separation guidelines.

Table 7: VLAN Separation Rules

If		Then
VLANSEP is “0” (Disabled),	**OR** the telephone is not tagging frames, **OR** the telephone is tagging frames with a VLAN ID equal to PHY2VLAN.	Frames received on the secondary Ethernet interface will not be changed before forwarding. For example, tagging is not added or removed and the VLAN ID and tagged frames priority are not changed. The Ethernet switch forwarding logic determines that frames received on the Ethernet line interface are forwarded to the secondary Ethernet interface or to the telephone without regard to specific VLAN IDs or the existence of tags.
VLANSEP is “1” (Enabled)		All tagged frames received on the secondary Ethernet interface are changed before forwarding to make the VLAN ID equal to the PHY2VLAN value and the priority value equal to the PHY2PRIO value. Untagged frames received on the secondary Ethernet interface are not changed before forwarding.
VLANSEP is “1” (Enabled)	**AND** the telephone is not tagging frames, **OR** if the telephone is tagging frames with a VLAN ID equal to PHY2VLAN, **OR** if the PHY2VLAN value is zero.	The Ethernet switch forwarding logic determines that frames received on the Ethernet line interface are forwarded to the secondary Ethernet interface or to the telephone without regard to specific VLAN IDs or the existence of tags.

1 of 2

Table 7: VLAN Separation Rules (continued)

If		Then
VLANSEP is “1” (Enabled)	**AND** the telephone is tagging frames with a VLAN ID not equal to PHY2VLAN, **AND** the PHY2VLAN value is not zero.	Tagged frames received on the Ethernet line interface will only be forwarded to the secondary Ethernet interface if the VLAN ID equals PHY2VLAN. Tagged frames received on the Ethernet line interface will only be forwarded to the telephone if the VLAN ID equals the VLAN ID used by the telephone. Untagged frames will continue to be forwarded or not forwarded as determined by the Ethernet switch forwarding logic.
		2 of 2

Unnamed Registration

As of Release 2.4, 4600 Series IP Telephones support unnamed registration. A telephone can register with the call server and receive limited service without requiring an extension and password entry. Unless otherwise disabled using the system value UNNAMEDSTAT, the telephone automatically attempts to register unnamed if no action is taken on the telephone **Extension** entry screen.

A telephone registered without the extension and password has the following characteristics:

- only one call appearance, preventing conferences or call transfers,
- no administrable feature buttons,
- on-hook dialing cannot be invoked,
- limited to the calling capability administered for PSA (Personal Station Access) on the call server, for example, only outgoing calls permitted subject to call server Class of Restriction/Class of Service limitations, and
- can be converted to normal, named registration by a valid extension and password entry.

IEEE 802.1X

As of Release 2.6, certain IP telephones support the IEEE 802.1X standard for pass-through and Supplicant operation. The system parameter DOT1X determines how applicable telephones handle 802.1X multicast packets and proxy logoff, as follows:

- When DOT1X = 0, the telephone forwards 802.1X multicast packets from the Authenticator to the PC attached to the telephone and forwards multicast packets from the attached PC to the Authenticator (multicast pass-through). Proxy Logoff is not supported.
- When DOT1X = 1, the telephone supports the same multicast pass-through as when DOT1X=0. Proxy Logoff is supported.
- When DOT1X = 2, the telephone forwards multicast packets from the Authenticator only to the telephone, ignoring multicast packets from the attached PC (no multicast pass-through). Proxy Logoff is not supported.
- Regardless of the DOT1X setting, the telephone always properly directs unicast packets from the Authenticator to the telephone or its attached PC, as dictated by the MAC address in the packet.

802.1X Pass-Through and Proxy Logoff

As of Release 2.2.3, IP telephones support pass-through of 802.1x packets to and from an attached PC. This enables an attached PC running 802.1x supplicant software to be authenticated by an Ethernet data switch.

As of Release 2.6, and as of Release 2.7 for the 4625SW, the IP Telephones support two pass-through modes:

- pass-through and
- pass-through with proxy logoff.

The DOT1X parameter setting controls the pass-through mode. In Proxy Logoff mode (DOT1X=1), when the secondary Ethernet interface loses link integrity, the telephone sends an 802.1X EAPOL-Logoff message to the data switch on behalf of the attached PC. The message alerts the switch that the device is no longer present. For example, a message would be sent when the attached PC is physically disconnected from the IP telephone. When DOT1X = 0 or 2, the Proxy Logoff function is not supported.

802.1X Supplicant Operation

As of Release 2.7, the 4602SW+ and 4625SW IP Telephones support Supplicant operation. As of Release 2.6, the 4610SW, 4620SW, 4621SW, and 4622SW IP Telephones support Supplicant operation.

IP telephones that support Supplicant operation also support Extensible Authentication Protocol (EAP), but only with the MD5-Challenge authentication method as specified in IETF RFC 3748 [8.5-33a].

A Supplicant identity (ID) and password of no more than 12 numeric characters are stored in reprogrammable non-volatile memory. The ID and password are not overwritten by telephone software downloads. The default ID is the MAC address of the telephone, converted to ASCII format without colon separators, and the default password is null. Both the ID and password are set to defaults at manufacture. EAP-Response/Identity frames use the ID in the Type-Data field. EAP-Response/MD5-Challenge frames use the password to compute the digest for the Value field, leaving the Name field blank.

When a telephone is installed for the first time and 802.1x is in effect, the dynamic address process prompts the installer to enter the Supplicant identity and password. The IP telephone does not accept null value passwords. See “Dynamic Addressing” in the *4600 Series IP Telephone Installation Guide*. The IP telephone stores 802.1X credentials when successful authentication is achieved. Post-installation authentication attempts occur using the stored 802.1X credentials, without prompting the user for ID and password entry.

An IP telephone can support several different 802.1X authentication scenarios, depending on the capabilities of the Ethernet data switch to which it is connected. Some switches may authenticate only a single device per switch port. This is known as single-supplicant or port-based operation. These switches typically send multicast 802.1X packets to authenticating devices.

These switches support the following three scenarios:

- **Standalone telephone (Telephone Only Authenticates) -** When the IP telephone is configured for Supplicant Mode (DOT1X=2), the telephone can support authentication from the switch.
- **Telephone with attached PC (Telephone Only Authenticates) -** When the IP telephone is configured for Supplicant Mode (DOT1X=2), the telephone can support authentication from the switch. The attached PC in this scenario gains access to the network without being authenticated.
- **Telephone with attached PC (PC Only Authenticates) -** When the IP telephone is configured for Pass-Through Mode or Pass-Through Mode with Logoff (DOT1X=0 or 1), an attached PC running 802.1X supplicant software can be authenticated by the data switch. The telephone in this scenario gains access to the network without being authenticated.

Some switches support authentication of multiple devices connected through a single switch port. This is known as multi-supplicant or MAC-based operation. These switches typically send unicast 802.1X packets to authenticating devices. These switches support the following two scenarios:

- **Standalone telephone (Telephone Only Authenticates) -** When the IP telephone is configured for Supplicant Mode (DOT1X=2), the telephone can support authentication from the switch.
- **Telephone and PC Dual Authentication -** Both the IP telephone and the connected PC can support 802.1X authentication from the switch. The IP telephone may be configured for Pass-Through Mode or Pass-Through Mode with Logoff (DOT1X=0 or 1). The attached PC must be running 802.1X supplicant software.

Link Layer Discovery Protocol (LLDP)

Release 2.6+ 4600 Series IP Telephones support IEEE 802.1AB. Link Layer Discovery Protocol (LLDP) is an open standards layer 2 protocol IP telephones use to advertise their identity and capabilities and to receive administration from an LLDP server. LAN equipment can use LLDP to manage power, administer VLANs, and provide some administration.

The transmission and reception of LLDP is specified in IEEE 802.1AB-2005. The 4600 Series IP Telephones use Type-Length-Value (TLV) elements specified in IEEE 802.1AB-2005, TIA TR-41 Committee - Media Endpoint Discovery (LLDP-MED, ANSI/TIA-1057), and Proprietary elements. LLDP Data Units (LLDPDUs) are sent to the LLDP Multicast MAC address (01:80:c2:00:00:0e).

A 4600 Series IP Telephone initiates LLDP after receiving an LLDPDU message from an appropriate system. Once initiated, the telephones send an LLDPDU every 30 seconds with the following contents:

Table 8: LLDPDU Transmitted by the 4600 Series IP Telephones

Category	TLV Name (Type)	TLV Info String (Value)
Basic Mandatory	Chassis ID	IPv4 IP Address of telephone.
Basic Mandatory	Port ID	MAC address of the telephone.
Basic Mandatory	Time-To-Live	120 seconds.
Basic Optional	System Name	The Host Name sent to the DHCP server in DHCP option 12.

1 of 3

Table 8: LLDPDU Transmitted by the 4600 Series IP Telephones (continued)

Category	TLV Name (Type)	TLV Info String (Value)
Basic Optional	System Capabilities	Bit 2 (Bridge) will be set in the System Capabilities if the telephone has an internal Ethernet switch. If Bit 2 is set in Enabled Capabilities then the secondary port is enabled. Bit 5 (Telephone) will be set in the System Capabilities. If Bit 5 is set in the Enabled Capabilities than the telephone is registered.
Basic Optional	Management Address	Mgmt IPv4 IP Address of telephone. Interface number subtype = 3 (system port). Interface number = 1. OID = SNMP MIB-II sysObjectID of the telephone.
IEEE 802.3 Organization Specific	MAC / PHY Configuration / Status	Reports autonegotiation status and speed of the uplink port on the telephone.
TIA LLDP MED	LLDP-MED Capabilities	Media Endpoint Discovery - Class III - IP Telephone.
TIA LLDP MED	Network Policy	Tagging Yes/No, VLAN ID for voice, L2 Priority, DSCP Value.
TIA LLDP MED	Inventory – Hardware Revision	MODEL - Full Model Name.
TIA LLDP MED	Inventory – Firmware Revision	BOOTNAME.
TIA LLDP MED	Inventory – Software Revision	APPNAME.
TIA LLDP MED	Inventory – Serial Number	Telephone serial number.
TIA LLDP MED	Inventory – Manufacturer Name	Avaya.
TIA LLDP MED	Inventory – Model Name	MODEL4 - 4 character name.

2 of 3

Table 8: LLDPDU Transmitted by the 4600 Series IP Telephones (continued)

Category	TLV Name (Type)	TLV Info String (Value)
Avaya Proprietary	PoE Conservation Level Support	Provides Power Conservation abilities/settings, Typical and Maximum Power values. OUI = 00-40-0D (hex), Subtype = 1.
Avaya Proprietary	Call Server IP Address	Call Server IP Address. Subtype = 3.
Avaya Proprietary	IP Phone Addresses	Phone IP Address, Phone Address Mask, Gateway IP Address. Subtype = 4.
Avaya Proprietary	CNA Server IP Address	CNA Server IP Address = in-use value from CNASRVR. Subtype = 5.
Avaya Proprietary	File Server	File Server IP Address. Subtype = 6.
Avaya Proprietary	802.1Q Framing	802.1Q Framing = 1 if tagging or 2 if not. Subtype = 7.
Basic Mandatory	End-of-LLDPDU	Not applicable.

3 of 3

On receipt of a LLDPDU message the Avaya IP Telephones will act on these Type-Length-Value (TLV) elements.

Table 9: Impact of TLVs on System Parameter Values

System Parameter Name	TLV Name	Impact
PHY2VLAN	IEEE 802.1 Port VLAN ID	System value changed to the Port VLAN identifier in the TLV.
L2QVLAN and L2Q	IEEE 802.1 VLAN Name	The system value is changed to the TLV VLAN Identifier. L2Q will be set to 1 (ON). VLAN Name TLV is only effective if: • The telephone is not statically programmed. • The telephone is not registered with the Call Server. • Name begins with VOICE (case does not matter). • The VLAN is not zero. If VLAN Name causes the telephone to change VLAN and the telephone already has an IP Address, the telephone will release the IP Address and send out a new DHCPDISCOVER on the new VLAN ID.
MCIPADD	Proprietary Call Server TLV	MCIPADD will be set to this value if it has not already been set.
TLSSRVR, HTTPSRVR and TFTPSRVR	Proprietary File Server TLV	TLSSRVR, HTTPSRVR and TFTPSRVR will be set to this value if none of them have already been set.
L2Q	Proprietary 802.1Q Framing	The default L2Q is set to the value of this TLV. No change is made to the current L2 tagging, but the new default value is used on the next reboot.
	Proprietary - PoE Conservation TLV	This proprietary TLV can initiate a power conservation mode. The telephones that support this will turn on/off the telephone backlight and the backlight of an attached EU24BL Button Module in response to this TLV.

These telephones:

- do not support LLDP on the secondary Ethernet interface.
- will not forward frames received with the 802.1AB LLDP group multicast address as the destination MAC address between the Ethernet line interface and the secondary Ethernet interface.

Administering Options for the 4600 Series IP Telephones

This chapter's Introduction indicates that there are many parameters you can administer for the 4600 Series IP Telephones. This section explains how to change parameters by means of the DHCP or TFTP/HTTP servers. In all cases, you are setting a system parameter in the telephone to a desired value. Table 10 lists the parameter names, their default values, the valid ranges for those values, and a description of each one. For DHCP, the DHCP Option sets these parameters to the desired values as discussed in DHCP Generic Setup on page 59. For TFTP and HTTP, the parameters in Table 10 are set to desired values in the Script File, as discussed in Contents of the Upgrade Script on page 78.

Avaya recommends that you administer options on the 4600 Series IP Telephones using script files. Some DHCP applications have limits on the amount of user-specified information. The administration required can exceed those limits, for example, for a 4630 with all applications administered.

You might choose to completely disable the capability to enter or change option settings from the dialpad, as of Release 1.8. As of that Release, a new system value, PROCPSWD, can be set as part of standard DHCP/TFTP administration. If PROCPSWD is non-null and consists of 1 to 7 digits, the user cannot invoke any "dialpad options" without first pressing **Mute** or **Hold** and entering the PROCPSWD value. See "Chapter 3" of the *4600 Series IP Telephone Installation Guide* for more information.

CAUTION:

PROCPSWD is likely stored on the server "in the clear" and is certainly sent to the telephone in the clear. Therefore, do not consider PROCPSWD as a high-security technique to inhibit a sophisticated end-user from obtaining access to local procedures.

Administering this password can limit access to all local procedures, including V I E W, which is read-only and would not change any settings in any case.

Note:

Parameters that do not specify "H.323" or "SIP" apply to both protocols.

Table 10: 4600 Series IP Telephone Customizable System Parameters

Parameter Name	Default Value	Description and Value Range
AGCHAND	1	Automatic Gain Control status for handset (0=disabled, 1=enabled).
AGCHEAD	1	Automatic Gain Control status for headset (0=disabled, 1=enabled).

1 of 12

Table 10: 4600 Series IP Telephone Customizable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
AGCSPKR	1	Automatic Gain Control status for Speaker (0=disabled, 1=enabled).
AUDIOENV	0	Audio environment selection index (0 to 107). Applies only to telephones with R2.4 or R2.6+ software. For more information, see Internal Audio Parameters on page 85.
AUDIOSTHD	0	Headset sidetone setting (0=No change, 1=6dB below nominal, 2=no sidetone - infinite loss). Applies only to telephones with R2.4 or R2.6 software.
AUDIOSTHS	0	Handset sidetone setting (0=No change, 1=6dB below nominal, 2=no sidetone - infinite loss). Applies only to telephones with R2.4 or R2.6 software.
AUTH	0	Script file authentication value (0=HTTP is acceptable, 1=HTTPS is required).
BAKLIGHTOFF	120	Number of minutes without activity to wait before turning off the display backlight. Values: 0-999, no spaces and no null value. A value of 0 means the backlight never turns off.
CALLFWDSTAT	0	Controls which Call Forwarding Feature Buttons are active and visible to the user for SIP telephones only. Valid value is one ASCII numeric digit, 0 to 7. Values are: 0 = No call forwarding 1 = Call Forward 2 = Call Forward Busy 3 = Call Forward and Call Forward Busy 4 = Call Forward No Answer 5 = Call Forward and Call Forward No Answer 6 = Call Forward Busy and Call Forward No Answer 7 = Call Forward, Call Forward Busy and Call Forward No Answer
CNAPORT	50002	Avaya Converged Network Analyzer (CNA) server registration transport-layer port number (0-65535). Applies only to H.323 telephones.
CNASRVR	“ ” (Null)	Text string containing the IP Addresses of one or more Avaya Converged Network Analyzer (CNA) servers, in dotted decimal or DNS format. Applies only to H.323 telephones.
COVERAGEADDR	“ ” (Null)	Call Coverage/Messages URI for SIP telephones. The URI used for **Call Coverage** and **Messages** buttons. Valid values are zero or one URI (0 to 255 ASCII characters). Null (“”) is a valid value, but the value may not contain spaces.

2 of 12

Table 10: 4600 Series IP Telephone Customizable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
CTISTAT	1	Computer-Telephony Integration (CTI) Status (1=enabled, 0=disabled). Applies only to H.323 telephones.
CTIUDPPORT	49721	CTI UDP listener port (49714 through 49721, inclusive). Applies only to H.323 telephones.
DATESEPARATOR	/	Date Separation Character for SIP telephones. Valid value is one ASCII graphic character from exclamation point (hex 21) through tilde (hex 7E). Null (“”) is not a valid value. The specified character is used to separate the month, day, and year on the telephone display.
DATETIMEFORMAT	0	Time/Date Display Format for SIP telephones. Valid value is one ASCII numeric digit, 0 to 3. The values and associated Time and Date format the SIP telephones display are: 0 = 12-hour time, mm/dd/yy 1 = 12-hour time, dd/mm/yy 2 = 24-hour time, mm/dd/yy 3 = 24-hour time, dd/mm/yy See Setting the Date and Time on SIP IP Telephones on page 110 for more information.
DHCPSTD	0	DHCP Standard flag. If set to “1” the telephone strictly follows the DHCP standard with respect to giving up IP Addresses when the DHCP lease expires. If set to “0” the telephone continues using the IP Address until it detects reset or a conflict (see DHCP Generic Setup).
DIALPLAN	“ ” (Null)	The Dial Plan for SIP telephones. Valid values are zero to 1000 of the following ASCII characters: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, *, #, x, Z, z, [,], -, +, |. See Setting the Dial Plan on SIP IP Telephones on page 110 for specific guidelines.
DIALWAIT	5	Dialing Timeout Interval for SIP telephones. Valid values are one or two ASCII numeric digits, 0 to 10. This parameter controls how many seconds the telephone waits after each dialable character is dialed. If an appropriate dial plan has not been defined, the SIP telephone assumes the number is complete and initiates a call when the timeout interval is reached.
DNSSRVR	" " (Null)	Text string containing the IP Address of one or more DNS servers, at least one of which must be a valid, non-zero, dotted decimal address.

3 of 12

Table 10: 4600 Series IP Telephone Customizable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
DOMAIN	" " (Null)	Text string containing the domain name to be used when DNS names in system values are resolved into IP Addresses.
DOT1X	0	802.1X Supplicant operation mode. Valid values are: 0=Unicast Supplicant operation only, with PAE multicast pass-through, but without proxy Logoff, 1=Unicast Supplicant operation only, with PAE multicast pass-through and proxy Logoff, 2=Unicast or multicast Supplicant operation, without PAE multicast pass-through or proxy Logoff.
DSTOFFSET	1	Daylight Savings Time Offset from Standard Time for SIP telephones. Valid value is one ASCII numeric digit, 0 to 2. The number of hours that clocks change between Standard Time and Daylight Savings Time.
DSTSTART	1SunApr2L	Daylight Savings Time Start Date for SIP telephones. Valid values are six, seven or nine ASCII characters with a format of either ***odddmmmht*** or ***Dmmmht***, where: **o** is 1 character representing an ordinal adjective as follows: 1 (first), 2 (second), 3 (third), 4 (fourth) or L (last); **ddd** is 3 characters containing the English abbreviation for the day of the week as follows: Sun, Mon, Tue, Wed, Thu, Fri or Sat; **mmm** is 3 characters containing the English abbreviation for the month as follows: Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov or Dec; **h** is 1 numeric digit representing the time at which to make the adjustment, exactly on the hour at hAM (0h00 in military format), where valid values of **h** are 0 through 9; **t** is 1 character representing the time zone relative to which to make the adjustment as follows: L (local time) or U (Universal Time); and, **D** is 1 or 2 ASCII digits representing the date of the month, from 1 or 01 to 31, or the character L, which means the last day of the month. For example, a value of “1SunApr2L” means “the first Sunday in April at 2AM local time,” and a value of “29Mar1U” means “March 29th at 1AM Universal Time.”
DSTSTOP	LSunOct2L	Daylight Savings Time Stop Date for SIP telephones. Valid values and format are the same as DSTSTART.

Table 10: 4600 Series IP Telephone Customizable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
ENHDIALSTAT	1	Enhanced Dialing Status. If set to “1” the Enhanced Local Dialing feature is turned on for all associated applications. If set to “0” the feature is turned off.
FTPSRVR	" " (Null)	IP Address of the FTP server on which an FTP backup/ restore file is stored. Format is dotted decimal or DNS name with from 0-255 ASCII characters, spaces not allowed. Not applicable to 4601 or 4602 IP Telephones.
FTPDIR	" " (Null)	FTP server directory path on which an FTP backup/ restore file is stored. Format is dotted decimal or DNS name with from 0-255 ASCII characters, with spaces allowed.
FTPUSERSTAT	1	Administered user permissions for FTP backup/restore files. Controls whether the user may specify an FTP server IP Address and/or directory path for backing up and restoring user data. Valid values are: 1=User can specify server and directory path. 2=User can specify directory path only. 0=User must use the server and directory path administered. If the telephone is supposed to restore/retrieve data with HTTP/HTTPS as indicated by the system value of BRURI, the system value of RESTORESTAT (and not FTPUSERSTAT) is the only relevant permission to backup/restore. This is because HTTP/HTTPS is invoked when BRURI is non-null, and if the operation fails, FTP is not attempted.
GMTOFFSET	0:00	Standard Time Offset from Greenwich Mean Time for SIP telephones. Valid values are a positive or negative number of hours and minutes less than 13 hours (1 to 6 ASCII characters, optionally beginning with “+” or “-”, followed by one or two ASCII numeric digits whose combined value is from 0 to 12, optionally followed by a “:” and two ASCII numeric digits whose combined value is from 00 to 59).
HEADSYS	1	Headset operational mode. One ASCII numeric digit. Valid values are: 0 or 2 - General Operation, where a disconnect messages returns the telephone to an idle state. 1 or 3 - Call Center Operation, where a disconnect message does not change the state of the telephone.

5 of 12

Table 10: 4600 Series IP Telephone Customizable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
ICMPDU	1	Internet Control Message Protocol Destination Unreachable transmission. Valid values are: 0 = Destination Unreachable (DU) messages are not transmitted. 1 = A Destination Unreachable (DU) message is not transmitted in response to received datagrams for which the designated transport protocol is not supported, or in response to datagrams that designate closed TCP ports. A DU message with a code of 3 (Port Unreachable) is transmitted only in response to datagrams designating closed UDP ports having port numbers greater than 32,767 and less than 35,000. 4600 Series IP Telephones might limit the number of such messages transmitted per second. Additional messages designating an unsupported transport protocol or port may be ignored. 2 = A Destination Unreachable (DU) message with a code of 2 (Protocol Unreachable) is transmitted if the designated transport protocol is not supported, and a DU with a code of 3 (Port Unreachable) is transmitted if a closed TCP or UDP port is designated. 4600 Series IP Telephones might limit the number of such messages are transmitted per second. Additional messages designating an unsupported transport protocol or port may be ignored.
ICMPRED	0	Internet Control Message Protocol Redirect message support. Valid values are: 0 = Received redirect messages are not supported. 1 = Received redirect messages supported. Note that redirect messages are never transmitted.
IRSTAT	1	Text string containing status of Infrared interface (0=off/disabled, 1=on/enabled).
L2Q	0	802.1Q framing value (0=auto, 1=on, 2=off).
L2QAUD	6	Layer 2 audio priority value (0 to 7).
L2QSIG	6	Layer 2 audio priority value (0 to 7).
L2QVLAN	0	802.1Q VLAN Identifier (0 to 4094).
MCPORT	1719	Media server transport-layer port number (0-65535). Applies only to H.323 telephones. Applies only to pre-2.6 software releases.

6 of 12

Table 10: 4600 Series IP Telephone Customizable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
MUSICSRVR	“ ” (Null)	Music Server IP Addresses for SIP telephones. Valid values are zero or more IP Addresses in dotted-decimal or DNS name format, separated by commas without any intervening spaces (0 to 255 ASCII characters, including commas). Null (“”) is a valid value, but the value may not contain spaces.
MWISRVR	“ ” (Null)	Message Waiting Server IP Addresses for SIP telephones. Valid values are zero or more IP Addresses in dotted-decimal or DNS name format, separated by commas without any intervening spaces (0 to 255 ASCII characters, including commas). Null (“”) is a valid value, but the value may not contain spaces.
OPSTAT	111	Options status flags. Consists of 3 “bits” where each digit represents a 0 (disabled/off) or 1 (enabled/on). When OPSTAT is set to **000**, all options are disabled and a user attempt to access the Options menu produces an error screen. Setting the first character to **0** (001, 010, or 011) disables the second Options menu screen, blocking user access to Personal Ringing, Contrast Control, Backup/Restore, Feature Button Labeling, PC Ethernet interface, and Select Display Language. Setting the second character to **0** (001, 100, or 101) removes View IP Settings and Network Audio Quality from the main Options screen, making these options unavailable to the user. Further, setting the second character to 0 also removes the IP Address from the Discovering... message the telephone displays while attempting to find a media server. Setting the third character to **0** (100, 010, or 110) removes the Logoff option from the main Options menu, making this feature unavailable to the user.
PHNCC	1	Telephone country code. The administered international country code for the location of the serving MultiVantage™ server. Range: 1-3 digits, from “1” to “999.”
PHNDPLENGTH	5	Telephone dial plan length. The length of the administered dial plan for the serving MultiVantage™ server. Range: 1 or 2 digits, from “3” to “10.”
PHNIC	011	Telephone international access code. The digits dialed to access public network international trunks from the serving Multi-Vantage™ server. Range: 1-4 digits.

7 of 12

Table 10: 4600 Series IP Telephone Customizable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
PHNLD	1	Telephone long distance access code. The digit dialed to access public network long distance trunks from the serving MultiVantage™ server. Range: 1 digit or " " (Null).
PHNLDLENGTH	10	Length of national telephone number. The number of digits in the longest possible national telephone number for the serving Avaya Media Server's location. Range: 1 or 2 digits, from "5" to "15."
PHNNUMOFSA	3	Number of Session Appearances for SIP telephones. Valid values are a single ASCII numeric digit, 1 to 5. The number of session appearances that will be supported on phones with larger displays. The 4602 and 4602SW always have 2 session appearances.
PHNOL	9	Outside line access code. The character(s) dialed to access public network local trunks from the serving Avaya Media Server. Range: 0-2 dialable characters, including " " (Null).
PHY1STAT	1	Ethernet line interface setting (1=auto, 2=10Mbps half-duplex, 3=10Mbps full-duplex, 4=100Mbps half-duplex, 5=100Mbps full-duplex).
PHY2PRIO	0	Layer 2 priority value for frames received on or forwarded to the secondary Ethernet interface. Set this parameter only when VLAN separation is enabled. Values are from 0-7.
PHY2VLAN	0	VLAN identifier used by frames received on or forwarded to the secondary Ethernet interface. Set this parameter only when VLAN separation is enabled. Value is 1-4 ASCII numeric digits from "0" to "4094." Null is not a valid value, nor can the value contain spaces. If this value is set by LLDP using the Port VLAN ID TLV value, it will not change regardless of settings from other sources. For more information, see Parameter Data Precedence.
PHY2STAT	1	Secondary Ethernet interface setting (0=Secondary Ethernet interface off/disabled, 1=auto, 2=10Mbps half-duplex, 3=10Mbps full-duplex, 4=100Mbps half-duplex, 5=100Mbps full-duplex).
PROCPSWD	" " (Null)	Text string containing the local (dialpad) procedure password (Null or 1-7 ASCII digits).
PROCSTAT	0	Local (dialpad) Administrative Options status (0=all Administrative Options are allowed, 1=only VIEW is allowed).

Table 10: 4600 Series IP Telephone Customizable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
PUSHCAP	222	Push capabilities - audio receive push value (hundreds), Web push value (tens), or Top Line value. Any values other than combinations of 0, 1, and/or 2 are treated as "0" (disabled). Values are 000 to 999, defined as: 0 = Push disabled. 1 = Normal only push allowed. 2 = Normal and/or barge-on push allowed. For example, if the value is “222” everything is allowed, if the value is “111” no barge-in is allowed, and the value 200 signifies both a normal and barge-in audio push, but not a Web or Top Line push.
PUSHPORT	80	Destination TCP port for the telephone’s HTTP server. Valid values are: 80 to 65535.
QKLOGINSTAT	1	Quick Login Status. Valid values are: 0=Delete H.323 registration password upon user logoff. 1=Retain H.323 registration password upon user logoff.
REGISTERWAIT	3600	SIP Re-registration Interval. The SIP registration expiration interval (in seconds) sent to the SIP registrar during registration. Valid values are 1 to 5 ASCII numeric characters from 0 to 65535. Null (“”) is not a valid value, and the value may not contain spaces.
RESTORESTAT	1	FTP backup/restore file status. If the telephone supports backup/restore and this value is set to "1" and system value FTPSRVR is non-null, automatic backup and restore proceeds upon completion of telephone registration. If set to "0" automatic backup/restore does not occur upon registration and must be initiated by the user.
RTCPMON	" " (Null)	Text string containing the 4-octet IP Address of the RTCP monitor currently in use.
RTCPMONPORT	5005	The port used to send RTCP information to the IP Address specified in the RTCPMON parameter.
SIPDOMAIN	“ ” (Null)	SIP Domain Name. Valid values are 0 to 255 ASCII characters. Null (“”) is a valid value, but the value may not contain spaces. The domain name used in the Contact header for SIP registration. For example, if the SIP domain is “avaya.com”, the Contact header sent to the SIP registrar for extension 1234 would be sip:1234@avaya.com.

9 of 12

Table 10: 4600 Series IP Telephone Customizable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
SIPPROXYSRVR	“ ” (Null)	SIP Proxy Server IP Addresses. Valid values are zero or more IP Addresses in dotted-decimal or DNS name format, separated by commas without any intervening spaces (0 to 255 ASCII characters, including commas). Null (“”) is a valid value, but the value may not contain spaces.
SIPPORT	5060	SIP Server Port Number. Valid values are 1 to 5 ASCII numeric characters from “0” to “65535”. Null (“”) is not a valid value, and the value may not contain spaces.
SIPREGISTRAR	“ ” (Null)	SIP Registrar IP Addresses. Valid values are zero or more IP Addresses in dotted-decimal or DNS name format, separated by commas without any intervening spaces (0 to 255 ASCII characters, including commas). Null (“”) is a valid value, but the value may not contain spaces.
SNMPADD	" " (Null)	Text string containing one or more allowable source IP Addresses for SNMP queries, in dotted decimal or DNS format, separated by commas, with up to 127 total ASCII characters. The Null default means that SNMP is disabled. Release 2.6 does not support SNMP unless SNMPADD is set to a non-null value. When non-null, the telephone accepts only SNMP queries from the IP Addresses in this parameter. See the note under SNMPSTRING.
SNMPSTRING	" " (Null)	Text string containing the SNMP community string (up to 32 ASCII characters). The Null default means that SNMP is disabled. Release 2.6 does not support SNMP unless SNMPSTRING is set to a non-null value. **Note:** SNMPSTRING cannot be set using Static Addressing (ADDR). As of R2.7, SNMPSTRING cannot be set on telephones programmed statically, therefore SNMP cannot be used on those telephones.
SNTPSRVR	“ ” (Null)	Simple Network Time Protocol (SNTP) Server IP Addresses for SIP telephones. Valid values are zero or more IP Addresses in dotted-decimal or DNS name format, separated by commas without any intervening spaces (0 to 255 ASCII characters, including commas). Null (“”) is a valid value, but the value may not contain spaces.
SPEAKERSTAT	2	Hands-Free Audio Operation for SIP IP telephones. Valid value is one ASCII numeric digit, 0 to 2, as follows: 0=No hands-free audio 1=One-way Speaker (monitor) 2=Two-way Speaker

Table 10: 4600 Series IP Telephone Customizable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
STATIC	0	Static programming override flag. If set to “0” static programming never overrides file server- (DHCP or TFTP) or call server-administered data. If set to “1” the file server (TFTPSRVR, HTTPSRVR, TLSSRVR) address is overridden with the statically programmed value. If set to “2” the call server (MCIPADD) address is overridden with the statically programmed value, the only non-DHCP settable value. If set to “3” both the file server and call server addresses are overridden by the statically programmed values. STATIC can only be usefully set in DHCP, and values 1 and 3 must be set via DHCP. STATIC = 1 allows local programming of individual telephones to use a different file server than the one commonly used by all telephones at the site. This is useful to test a different set of 46xxsettings.txt parameters or to force a telephone to use a different software load than is commonly used. STATIC = 2 allows individual telephones to be programmed to go to one particular call server. STATIC = 3 provides the combined features of STATIC = 1 and STATIC = 2.
SYSLANG	English	Language of the 4610SW/4620/4620SW, 4621SW, 4622SW, and 4625SW user interface, in ASCII, independent of the MultiVantage™ message language. Options are English, Deutsche, Espanol, Francais, Italiano, Nederlands, Portugues and Katakana (Japanese). In addition to these languages, the 4610SW, 4620SW, and 4625SW also support (simplified) Chinese, Korean, Russian, and Hebrew. The 4610SW and 4620SW also support Japanese (Kanji).
TLSSRVR	" " (Null)	Text string containing the IP Addresses of one of more Avaya HTTPS servers, in dotted decimal or DNS format.
UNNAMEDSTAT	1	Unnamed Registration Status. Specifies whether unnamed registration is initiated if a user fails to enter a value at the *Password:* prompt. Valid values are: 0=Off 1=On For more information, see Unnamed Registration.
VLANSEP	1	VLAN separation. Controls whether frames to/from the secondary Ethernet interface receive IEEE 802.1Q tagging treatment. The tagging treatment enables frames to be forwarded based on their tags in a manner separate from telephone frames. If tags are not changed, no tag-based forwarding is employed. Values are: 1=Change tags as necessary, 2= Do not change tags.

11 of 12

Table 10: 4600 Series IP Telephone Customizable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
VLANTEST	60	Number of seconds to wait for a DHCPOFFER when using a non-zero VLAN ID (1-3 ASCII digits, from “0” to “999”).
WMLIDLETIME	10	The number of minutes until the browser sends an HTTP GET command for the URI specified in WMLIDLEURI. 1 to 3 ASCII numeric digits. Valid values are "1" to "999".
WMLIDLEURI	" " (Null)	The URI of the Web page displayed when WMLIDLETIME is reached and the HTTP GET is successful.

12 of 12

Note:

The 4630/4630SW and 4620/4620SW/4621SW/4622SW/4625SW IP Telephones have additional, optional administration. See Customizing the 4630/4630SW IP Telephone on page 111 and Customizing 4610SW, 4620/4620SW, 4621SW, 4622SW, and 4625SW IP Telephones on page 116 for more information.

DNS Addressing

As of Release 1.5, the 4600 IP Telephones support DNS addresses and dotted decimal addresses. The telephone attempts to resolve a non-ASCII-encoded dotted decimal IP Address by checking the contents of DHCP Option 6. See DHCP Generic Setup on page 59 for information. At least one address in Option 6 must be a valid, non-zero, dotted decimal address, otherwise, DNS fails. The system parameter **DOMAIN’s** (Option 15, Table 10) text string is appended to the address(es) in Option 6 before the telephone attempts to resolve the DNS address. If Option 6 contains a list of DNS addresses, those addresses are queried in the order given if no response is received from previous addresses on the list. As an alternative to administering DNS by DHCP, you can specify the DNS server and/or Domain name in the TFTP or HTTP script file. But first **SET** the **DNSSRVR** and **DOMAIN** values so you can use those names later in the script.

Note:

If you administer Options 6 and 15 appropriately with DNS servers and Domain names respectively, you do not need to specify **MCIPADD** and **TFTPSRVR** settings in the Site Specific Option string.

Customizing the Site-Specific Option Number (SSON)

DHCP Generic Setup on page 59, discusses that the SSON can be set to a string. For each system parameter listed in Table 10 that you want to include, append the SSON string with:

a comma followed by ***name=value***
where ***name*** is a parameter name and ***value*** is its associated value. Invalid values cause the data to be ignored for that name. Customizing the SSON affects all telephones associated with that DHCP server.

Entering Options Using the Telephone Dialpad

Local administrative procedures of note to LAN Administrators might be:

- QoS Option Setting - to customize any or all of the QoS parameters locally.
- Secondary Ethernet (Hub) Interface Enable/Disable - to enable or disable the secondary Ethernet hub locally.
- Reset - to return all system initialization values to the application software default values, see The Reset Administrative Option on page 132.
- View - to view the 4600 IP Telephone system parameters, see The View Administration Option on page 135.
- Clear - to remove *all* administered values, user-specified data, and option settings, etc, see The Clear Administrative Option on page 130.
- Restart -to restart a particular telephone, see Restart the Telephone on page 134.

Chapter 3 of the *4600 Series IP Telephone Installation Guide* details how to use all local administrative options.

Enhanced Local Dialing

The 4610SW, 4620/4620SW, 4621SW, 4622SW, 4625SW, and 4630/4630SW have a variety of telephony-related applications (e.g., Speed Dial, Call Log, Web Browser, etc.). These applications might obtain a telephone number during operation. For example, the Call Log saves an incoming caller’s number, while the Web browser might obtain a dialable link from a corporate Web site. Before Release 1.8 software, when the user indicated a desire to call one of these incoming numbers, the 4610SW/4620/4620SW/4630/4630SW would first require the user to edit the number, generally by prepending digits to account for dial access codes, country codes if applicable, etc.

As of Release 1.8, the 4610SW/4620/4620SW/4630/4630SW can evaluate a raw telephone number. This is also true of the 4621SW, 4622SW, and 4625SW as of Release 2.2. Based on administered parameters, the telephone can automatically prepend the correct digits, saving the user time and effort. This is the “Enhanced Dialing” feature. The key to this feature’s success is accurate administration of several important values. Table 12 summarizes these values and their meanings. That information is expanded upon in this section.

Note:

In all cases, the values you administer are the values relevant to the Avaya Media Server’s location at which the IP telephones are registered. If a telephone is in Japan, but its media server is in the United States, set the **PHNCC** value to “1" for the United States.

In all cases, the digits the phones insert and dial are subject to standard Avaya Media Server features and administration. This includes Class of Service (COS), Class of Restriction (COR), Automatic Route Selection (ARS), etc.

As indicated in Table 10, you can administer the system parameter **ENHDIALSTAT** to turn off the Enhanced Local Dialing feature.

The system values relevant to the Enhanced Dialing Feature are:

- **PHNCC -** the media server’s international country code.
  For example, “1” for the United States, “44” for the United Kingdom, etc.
- **PHNDPLENGTH -** the length of the dial plan on the media server.
- **PHNIC -** the digits the media server dials to access public network international trunks.
  For example, “011” for the United States.
- **PHNLD -** the digit dialed to access public network long distance trunks on the media server.
- **PHNLDLENGTH -** the maximum length, in digits, of the national telephone number for the country in which the Avaya Media Server is located.
- **PHNOL -** the character(s) dialed to access public network local trunks on the media server.

Example: A corporate voice network has a 4-digit dialing plan. The corporate WML Web site lists a 4-digit telephone number as a link on the Human Resources page. A 4620 user selects that link. The 4620 deduces the telephone number is part of the corporate network because the telephone number’s length is the same as the corporate dialing plan. The telephone dials the number without further processing.

Example: A user notes a Web site contains an international telephone number that needs to be called, and presses “Call.” The 4630/4630SW determines the number to be called is from another country code. The telephone then prepends the rest of the telephone number with PHNOL to get an outside line + PHNIC to get an international trunk. The 4630/4630SW then dials normally, with the Avaya Media Server routing the call appropriately.

Note:

The Enhanced Local Dialing algorithm requires that telephone numbers be presented in a standard format. The standard format depends on how you administer the parameters indicated in Table 12. The algorithm also assumes that international telephone numbers are identified as such in, for example, WML Web sites. This is indicated by preceding that type of number with a plus (+) sign, and a space or some non-digit character following the country code.

Setting the Date and Time on SIP IP Telephones

SIP IP telephones need a source of date and time information. This typically comes from a network time server running the Simple Network Time Protocol (SNTP). The telephones use several administrative parameters for this functionality. The parameter SNTPSRVR defines the server's IP Address(es). GMTOFFSET defines the offset from Greenwich Mean Time (GMT). DSTSTART and DSTSTOP define the start and end of Daylight Savings Time, respectively. DSTOFFSET defines the Daylight Savings Time offset from Standard Time. Finally, DATETIMEFORMAT defines the format of the date and time display. See Table 10 for definitions and valid values for SIP Date and Time parameters.

Setting the Dial Plan on SIP IP Telephones

A dial plan is used during manual dialing to allow a call to be initiated without using a **Send** button and without waiting for the expiration of a timeout interval. The dial plan consists of one or more format strings separated by the logical OR symbol (I). When the dialed digits match a format string in the dial plan, the call is initiated. The DIALPLAN parameter defines the dial plan.

Valid characters in a format string, and their meanings, are as follows:

digits 0 through 9, inclusive = Specific dialpad digits
***** = the dialpad character *
# = the dialpad character # (but only if it is the first character in the dialed string – see below)
x = any dialpad digit (i.e., 0-9)
Z or **z** = present dial tone to the user (for example, for Feature Access Code (FAC) entry)
[ ] = any one character within the brackets is a valid match for a dial plan string
- = any one digit between the bounds within the brackets, inclusive, is a match
+ = the character preceding the + can repeat 0 or more additional times, for a valid match

Dial plan example:

"[2-4]xxx|[68]xxx|*xx|9Z1xxxxxxxxxx|9z011x+"

where:

[2-4]xxx: Four-digit dial extensions, with valid extensions starting with 2, 3, or 4;

[68]xxx: Four-digit dial extensions, with valid extensions starting with 6 or 8;

*xx: Two-digit Feature Access Codes, preceded by a *;

9Z1xxxxxxxxxx: Network Access Code ("9 for an outside line"), followed by dial tone, followed by any string of 10 digits– typical instance of Automatic Route Selection (ARS) for standard US long distance number;

9z011x+: Network Access Code ("9 for an outside line"), followed by dial tone, followed by at least one digit – typical instance of Automatic Route Selection (ARS) for US access to international numbers of unknown, and variable, length.

Table 10 provides definitions and valid values for each SIP dial plan parameter.

Customizing the 4630/4630SW IP Telephone

The 4630/4630SW IP Telephone has some unique and powerful capabilities that take advantage of its large display and access to LAN facilities. If your LAN has an LDAP-compliant directory, or if you have a corporate Web site suitable for the 4630's/4630SW's 1/4-VGA display, the telephone needs key information about the servers providing those facilities. Specifically, to administer the 4630/4630SW Telephone for the LDAP Directory application or the Web Access application, you must provide the information Table 11 calls for. You must provide this information in a customized script file, in accordance with 4600 Series IP Telephone Scripts and Application Files on page 74.

CAUTION:

For the 4630/4630SW to work properly, you must have a 46xxsettings.scr or 46xxsettings.txt file in the same directory as the 4630/4630SW application file. If you do not edit the 46xxsettings file, the 4630/4630SW uses default settings only. The 46xxsettings file is no longer part of the *.zip file on the Avaya software download Web site, but is available as a stand-alone download. If you already have such a file because you downloaded it for a previous 4630 release, installing the stand-alone file overwrites the original file.

Note:

The 4620 and the 4630/4630SW IP Telephones use the same ***46xxsettings*** file.

In Table 11, parameters shown with a *Mandatory* status must be accurate and non-null for the application to work. The Avaya Help Web site, however, is always available. Parameters with an **Optional** status may be changed to suit your environment. If you do not change the parameters, their defaults are used.

Table 11: 4630/4630SW IP Telephone Customizable System Parameters by Application

Parameter Name	Default Value	Status	Description and Value Range
Phone Application Parameters:			
PHNEMERGNUM	" " (Null)	Optional	Text string of a telephone number to be dialed in case of an emergency (e.g., 911).
Directory Application Parameters:			
DIRSRVR	" " (Null)	Mandatory	Text string of dotted decimal IP Address, or DNS name, of the server containing the LDAP directory.
DIRTOPDN	" " (Null)	Mandatory	“Directory Topmost Distinguished Name.” Text string of the LDAP directory’s root entry. Note that spaces and other special characters might need to be treated as specified in RFC 2253, *Lightweight Directory Access Protocol (v3); UTF-8 String Representation of Distinguished Names.*
DIRFULLNAME	cn	Optional	Text string for the database field’s customer-specific label.
DIRTELNUM	telephoneNumber	Optional	Text string for the customer-specific label for the database field containing telephone numbers. The default is the standard LDAP value.
DIRSRCHTIME	0	Optional	Text string for an integer number of seconds. This is the maximum duration the LDAP directory spends searching before reporting completion or failure of the search. The default is LDAP-standard for “unlimited duration.”
DIRLDAPPORT	389	Optional	Directory LDAP Port. The port that exchanges LDAP messages with the server.
Stock Ticker Application Parameters:			
STKSTAT	1	Optional	Text string identifying whether the phones are allowed to have the Stock Ticker Application. “1” is the default and “0” disables the Stock Ticker Application.
Voice Mail Application Parameters:			
VMLHOME	" " (Null)	Mandatory	Text string containing the URL of the home page for the Voice Mail Application.

1 of 2

Table 11: 4630/4630SW IP Telephone Customizable System Parameters by Application (continued)

Parameter Name	Default Value	Status	Description and Value Range
Web Access Application Parameters:			
WEBHOME	" " (Null)	Mandatory	Text string containing the URL of the home page for the Web Access application.
WEBPROXY	" " (Null)	Optional	Text string containing the IP Address, in dotted decimal or DNS format, of an HTTP proxy server. This parameter is optional if the all the Web pages the user accesses are on your organization's intranet.
WEBEXCEPT	" " (Null)	Optional	Text string containing a list of one or more HTTP proxy server exception domains. Separate each exception with commas, and use up to a total of 127 ASCII characters. This parameter is optional if all the Web pages the user accesses are on your organization's intranet. If WEBPROXY is null, the value of this parameter is ignored.
WEBPORT	80	Optional	Text string containing the TCP port number for the HTTP proxy server. The default is the TCP default for HTTP. This parameter is optional if all the Web pages the user accesses are on your organization's intranet. If WEBPROXY is null, the value of this parameter is ignored.

2 of 2

Note:

For assistance in developing local Web sites tailored to the 4630 IP Telephone's display, see Appendix B: Creating Web Sites for the 4630/4630SW IP Telephone.

4630/4630SW Backup/Restore

4630/4630SW users can create an FTP backup file for Speed Dial button labels and unique option or parameter settings. The associated Option is covered in Chapter 8 of the *4630/4630SW IP Telephone User Guide*. Data is saved in a file called **4630data.txt** on a user-specified server and in a user-specified directory. Unlike the 4620/4620SW settings indicated in Table 12, the 4630/4630SW FTP settings cannot be centrally administered.

In addition to Speed Dial labels and associated telephone numbers, a backup saves these options and non-password parameters:

Setting/Parameter Name	Type
Idle Timeout	Option
Keyboard Layout	Option
Click Feedback	Option
Edit Dialing	Option
Personalized Ring	Option
Redial	Option
Go to Phone on Incoming Calls	Option
Go to Phone on Originate	Option
Call Timer	Option
Alphabetize Entries?	Option
Call Log Active?	Option
Call Log Automatic Archive	Option
Directory User ID	Parameter
Automatic Backup	Option
FTP Server IP Address	Parameter
FTP Directory Path	Parameter
FTP User ID	Parameter
Stock Ticker Active?	Option
STK.*mm*	Parameter
Stock Index DJIA	Option
Stock Index S&P 500	Option
Stock Index Nasdaq	Option
Stock Change	Option
Stock Volume	Option

If the Automatic Backup option is set to **No**, Speed Dial data, Options and Parameter settings are not saved. However, the user can force a one-time backup via the appropriate option. See Chapter 8 of the *4630 IP Telephone User Guide* for information. Restoring backed-up data is a separate user option, also covered in Chapter 8 of the *4630 IP Telephone User Guide.*

Note:

For specific error messages relating to Backup/Restore, see Table 17: Possible Error Messages During 4610SW, 4620/4620SW, 4621SW, 4622SW, 4625SW, and 4630/4630SW Backup/Restore on page 145.

Call Log Archive

Automatic archiving of the Call Log occurs when:

- The Call Log Automatic Archive option setting is **Yes,** and
- The Call Log is more than 50% filled with unarchived entries. Or, when a new (unarchived) log entry occurs within two hours of the last archive (whichever occurs first).

Call Log Archive automatically saves applicable Call Log entries. When the Call Log Automatic Archive option on a 4630/4630SW IP Telephone is set to **Yes** and the FTPSRVR is specified, the **`FTP APPE`** command attempts to save all call log contents to the FTP server. The FTP Server is the FTPSRVR value in the FTPDIR directory path. The file **4630calllog.txt** saves the data. The System Administrator can optionally specify **FTPSRVR** and/or **FTPDIR** by network administration. However, the telephone user can also specify these values. Chapter 8 of the *4630/4630SW IP Telephone User Guide* covers user specification. Automatic backup occurs whenever the user executes a **`Save`** command on a Speed Dial or Options/Parameter screen.

Note:

For specific error messages relating to Archiving, see Table 17: Possible Error Messages During 4610SW, 4620/4620SW, 4621SW, 4622SW, 4625SW, and 4630/4630SW Backup/Restore on page 145.

Customizing 4610SW, 4620/4620SW, 4621SW, 4622SW, and 4625SW IP Telephones

The 4610SW/4620/4620SW/4621SW/4622SW/4625SW IP Telephones have some unique and powerful capabilities that take advantage of their display and access to LAN facilities. If your LAN has an LDAP-compliant directory or a WML Web site, the telephone needs key information about the servers providing those facilities. Specifically, you need to provide the information relevant sections of Table 12 call for. You must provide this information in a customized script file, in accordance with 4600 Series IP Telephone Scripts and Application Files on page 74.

CAUTION:

For a 4610SW, 4620/4620SW, 4621SW, 4622SW, or 4625SW to work properly, you must have a 46xxsettings.txt file in the same directory as the 4610SW/4620/4620SW/4621SW/4622SW/4625SW application file. If you do not edit the 46xxsettings.txt file, those telephones use default settings only. The 46xxsettings file is no longer part of the *zip file on the Avaya software download Web site, but is available as a stand-alone download. If you already have such a file because you downloaded it for a previous 4610SW, 4620/4620SW, 4621SW, 4622SW, or 4625SW IP Telephone release, installing the stand-alone file overwrites the original file.

Note:

The 4610SW/4620/4620SW and the 4630/4630SW IP Telephones use the same ***46xxsettings.txt*** file.

In Table 12, parameters shown with a **Mandatory** status must be accurate and non-null for the application to work. You can change parameters with an **Optional** status to suit your environment. If you do not change parameters, their defaults are used.

Table 12: 4610SW, 4620/4620SW, 4621SW, 4622SW, and 4625SW IP Telephone Customizable System Parameters

Parameter Name	Default Value	Status	Description and Value Range
General User Parameters:			
APPSTAT	1	Optional	Applications status flag. See The Application Status Flag (APPSTAT) on page 119 for a description. See Table 13 for the range of values.
FTPDIR	" " (Null)	Optional	FTP Server Directory. The path on the FTP server to the directory in which an FTP backup/restore is saved.

Table 12: 4610SW, 4620/4620SW, 4621SW, 4622SW, and 4625SW IP Telephone Customizable System Parameters (continued)

Parameter Name	Default Value	Status	Description and Value Range
FTPUSERSTAT	1	Optional	FTP User Permission. If set to “0” the user **cannot** specify alternatives to the FTP servers and FTP directories DHCP and/or TFTP/HTTP administration specify. If set to “1” the user **can** specify alternatives to the FTP servers and FTP directories that DHCP and/or TFTP/HTTP administration specify. If set to “2” the user **cannot** specify alternatives to the FTP servers that DHCP and/or TFTP/HTTP administration specify, but **can** specify alternatives to FTP Directories.
PUSHCAP	222		Push capabilities - audio receive push value (hundreds), Web push value (tens), or Top Line value. Any values other than combinations of 0, 1, and/or 2 are treated as "0" (disabled). Values are 000 to 999, defined as: 0 = Push disabled. 1 = Normal only push allowed. 2 = Normal and/or barge-on push allowed. For example, if the value is “222” everything is allowed, if the value is “111” no barge-in is allowed, and the value 200 signifies both a normal and barge-in audio push, but not a Web or Top Line push.
PUSHPORT	80		Destination TCP port for the telephone’s HTTP server. Valid values are: 80 to 65535.
SYSLANG	English	Optional, and can be user-specified	Language of the 4610SW/4620/4620SW, 4621SW, 4622SW, and 4625SW user interface, in ASCII, independent of the MultiVantage™ message language. Options are English, Deutsche, Espanol, Francais, Italiano, Nederlands, Portugues and Katakana (Japanese). In addition to these languages, the 4610SW, 4620SW, and 4625SW also support (simplified) Chinese, Korean, Russian, and Hebrew. The 4610SW and 4620SW also support Japanese (Kanji).
UNNAMEDSTAT	1	Optional	Unnamed Registration Status. Specifies whether unnamed registration is initiated if a user fails to enter a value at the *Password:* prompt. Valid values are: 0=Off 1=On For more information, see Unnamed Registration.

2 of 4

Table 12: 4610SW, 4620/4620SW, 4621SW, 4622SW, and 4625SW IP Telephone Customizable System Parameters (continued)

Parameter Name	Default Value	Status	Description and Value Range
Web Access Application Parameters:			
SUBSCRIBELIST	" " (Null)	Optional	Subscription list for potential pushed content. List of zero or more fully qualified URLs, separated by commas without intervening spaces, with up to 255 total characters. See Appendix E: The Push Feature.
TPSLIST	" " (Null)	Optional	List of Trusted Push Servers. List of zero or more fully qualified domain/path strings, separated by commas without intervening spaces, with up to 255 total characters. See Appendix E: The Push Feature.
WMLEXCEPT	" " (Null)	Optional	Text string containing a list of one or more HTTP proxy server exception domains, separated by commas, up to a total of 127 ASCII characters. This parameter is optional if the Web pages to be accessed by the user are all on your organization's intranet. If WMLPROXY is null, the value of this parameter is ignored.
WMLHOME	" " (Null)	Mandatory	Text string containing the URL of the home page for the Web Access application.
WMLIDLETIME	10	Optional	The number of minutes until the browser sends an HTTP GET command for the URI specified in WMLIDLEURI. 1 to 3 ASCII numeric digits. Valid values are "1" to "999".
WMLIDLEURI	" " (Null)	Optional	The URI of the Web page displayed when WMLIDLETIME is reached and the HTTP GET is successful.
WMLPORT	80	Optional	Text string containing the TCP port number for the HTTP proxy server. The default is the TCP default for HTTP. This parameter is optional if the Web pages to be accessed by the user are all on your organization's intranet. If WMLPROXY is null, the value of this parameter is ignored.
WMLPROXY	" " (Null)	Optional	Text string containing the IP Address, in dotted decimal or DNS format, of an HTTP proxy server. This parameter is optional if the Web pages a user accesses are all on your organization's intranet.

3 of 4

Table 12: 4610SW, 4620/4620SW, 4621SW, 4622SW, and 4625SW IP Telephone Customizable System Parameters (continued)

Parameter Name	Default Value	Status	Description and Value Range
Backup/Restore Parameters			
FTPSRVR	" " (Null)	Mandatory but can be user-specified	Text string containing the 4-octet IP Address for the FTP server that stores and retrieves 4610SW/4620/4620SW/4621SW/4622SW/ 4625SW user information. See The Application Status Flag (APPSTAT) on page 119.
RESTORESTAT	1	Mandatory, but can be user-specified	FTP backup/restore file status. If the telephone supports backup/restore and this value is set to "1" and system value FTPSRVR is non-null, automatic backup and restore proceeds upon completion of telephone registration. If set to "0" automatic backup/restore does not occur upon registration.
Backlight Parameters			
BAKLIGHTOFF	120	Optional	Number of idle minutes after which the backlight turns off (1-3 ASCII digits, from 0-999).

Note:

Appendix C: Creating Web Sites for Other 4600 Series IP Telephones provides assistance in developing local Web sites tailored to applicable IP Telephone displays.

The Application Status Flag (APPSTAT)

The 4610SW, 4620/4620SW, 4621SW, 4622SW, and 4625SW IP Telephones offer the user numerous applications like Speed Dial, Call Log, Redial, etc. Each of these applications allows the user to add, delete, or in some cases, edit entries. However, you as the administrator may not want the user to have that level of functionality. For example, a hotel lobby telephone probably should not allow a user to delete the concierge's Speed Dial number. Further, for privacy reasons, that same telephone should not allow a Call Log display. You can use the Application Status Flag, APPSTAT, to administer specific application functionality permission levels for one or more telephones.

APPSTAT consists of one number, specifying a certain level of allowed functionality. A Zero ("0") value is the most limiting setting. Values "2" and "3" allow increasing levels of functionality, and "1" allows the user complete application functionality.

Table 13: Application Status Flags and Their Meaning

APPSTAT Value	Meaning
0	Redial and Call Log are suppressed. Speed Dial changes are not allowed.
1	***All administered applications are displayed, with full functionality. This is the default value.***
2	Call Log is suppressed. Speed Dial changes are not allowed. Only one-number Redial is allowed.
3	Speed Dial changes are not allowed.

In Table 13, “suppressed” applications are not displayed to the user. Softkey labels, application tabs, etc. that would usually be labeled or displayed to indicate the presence of that application are not labeled or displayed. Options associated with suppressed applications can continue to display unless overridden by appropriate OPSTAT parameter administration. However, displayed options have no effect while the application is suppressed.

In Table 13, “Speed Dial changes are not allowed” means the Speed Dial application displays and the user can make calls as normal. However, any controls that allow the user to change any aspect of the Speed Dial application do not display. This restriction includes the ability to add, delete, or edit any Speed Dial name or number.

In Table 13, “Only one-number Redial is allowed” means the user Option that allows a choice between displaying one, three, or six of the last numbers dialed, depending on the telephone, is suppressed. The Redial buffer stores only one number. The Redial application does not display since the user can redial only one number. This restriction allows a certain measure of privacy once a given user has left the telephone.

Note that you can:

- set **APPSTAT** to **1**, for example, in a staging area,
- administer a given telephone with Speed Dial entries of your choice, like the **Concierge Speed Dial** button in an earlier example,
- then move the telephone to where it will be used, where you have administered APPSTAT to be, say, 0 (zero).

When the relocated telephone resets, it retains its Speed Dial entries, like Concierge, but does not allow the user to create new entries.

When you set APPSTAT to any valid value other than 1, the telephone does not accept any Speed Dial button label changes that might have been made directly on an FTP backup file. Only the telephone’s existing labels are used. This restriction prevents circumvention of the APPSTAT restrictions.

APPSTAT has no effect on telephones having no user-selectable applications such as the 4602. Also, to “suppress” the WML applications, all you have to do is not administer the appropriate parameters. In essence, these applications are suppressed by default.

Backup/Restore for 4610SW, 4620/4620SW, 4621SW, 4622SW and 4625SW IP Telephones

Backup/Restore automatically saves Speed Dial button labels, and options/parameter settings, including local Feature button labels. For the 4625SW IP Telephone, backup also stores the background color of the Phone, Speed Dial, Call Log, and Options applications.

When the Automatic Backup option on a 4610SW, 4620/4620SW, 4621SW, 4622SW, or 4625SW IP Telephone is set to **Yes** and **FTPSRVR** is specified, the **`FTPSTOR`** command attempts to save all Speed Dial contents, all system options, and non-password parameters to the FTP server specified by **FTPSRVR**.

For H.323 telephones, data is saved in a text file called ***ext*_4610data.txt** or ***ext*_4620data.txt**, as appropriate to the telephone type, where ***ext*** stands for the telephone extension. For SIP telephones, data is saved in a text file called ***ext*_4610data_sip.txt** or ***ext*_4620data_sip.txt**, as appropriate to the telephone type. The 4621SW, 4622SW, and 4625SW all use “4620” as the telephone type for purposes of the Backup/Restore filename, to allow seamless upgrades from 4620s if applicable.

The system administrator can optionally set the backup option and specify **FTPSRVR** through network administration. A telephone user can also specify these values, as covered in Chapter 6 of the appropriate User Guide for the telephone type. Automatic backup occurs whenever the user executes a **`Save`** command on a Speed Dial or Options/Parameter screen.

Note:

Users can specify alternate servers and directories, for example, their own PCs, for backups and retrievals.

The 4610SW/4620/4620SW/4621SW/4622SW/4625SW backup/restore file can contain ASCII, Extended ASCII, and non-ASCII characters. However, if the file contains non-ASCII characters, specifically Cyrillic, Hebrew, Katakana, Han, or Hiragana characters, the file must be stored in UTF-8 form. The 4610SW/4620/4620SW/4621SW/4622SW/4625SW creates a file in this form automatically. But if you opt to create a backup/restore file yourself or edit this file, you must do both of the following:

1. Insert a blank line at the beginning of the file, and
2. Save the file in UTF-8 format.

These precautions ensure that regardless of how your editor stores the data file, the telephone can read the contents. If you fail to insert the blank line, the first line of data might be ignored. The 4620 does not support displays of Cyrillic, Hebrew, Han, or Hiragana characters. Even the 4610SW/4620SW/4621SW/4622SW/4625SW cannot support all Han or Hiragana characters. If you insert a character that the 4610SW/4620SW/4621SW/4622SW4625SW does not support, the display shows that character as a rectangle.

In addition to Speed Dial labels and associated telephone numbers, the following options, settings and non-password parameters are saved during a backup:

Setting/Parameter Name	Type
Personalized Ring	Option
Redial	Option
Phone Screen on Answer	Option
Phone Screen on Calling	Option
Call Timer	Option
Message Display Rate	Option
Call Appearance Width	Option (4620/4620SW, 4621SW, 4622SW, and 4625SW only; H.323 only)
Visual Alerting	Option
Call Log Enable	Option
Contrast	Option
Display Language	Option
Ethernet	Option
Automatic Backup	Option
FTP Server IP Address	Parameter
FTP Directory Path	Parameter
FTP User Name	Parameter
Phone Application Background Color	Setting (4625SW only)
Speed Dial Application Background Color	Setting (4625SW only)
Call Log Application Background Color	Setting (4625SW only)
Options Application Background Color	Setting (4625SW only)
Session Appearance Width	Option (SIP only)
Transfer Type	Option (SIP only)

Note:

When the Options Status Flag, **OPSTAT**, is set to **0** or **000**, retrieving backed up data has no effect. This prevents a user from bypassing the administration of OPSTAT and changing options settings in the backup file. Table 12 includes OPSTAT values.

Chapter 5: Troubleshooting Guidelines

Introduction

This chapter describes problems that might occur during 4600 Series IP Telephone operation and possible ways of resolving these problems.

Error Conditions

Table 14: Some Error Conditions in Operation of 4600 Series IP Telephones identifies some of the possible operational problems that might be encountered after successful 4600 Series IP Telephone installation. Possible installation problems and how to conduct a telephone self-test are discussed in the *4600 Series IP Telephone Installation Guide's* "Troubleshooting" chapter. The User Guides available on the Avaya support Web site also contain guidance for users having problems with specific IP telephone applications.

Note:

Most of the problems reported by 4600 Series IP Telephone users are not likely to be problems with the telephone itself. Problems are more likely LAN-based, where Quality of Service, server administration, and other issues can impact end-user perception of IP telephone performance.

Most error conditions are related to network problems, and are common to both SIP and H.323 telephones. Unless otherwise stated, the error conditions and messages covered in this chapter apply equally to both telephone types (H.323 and SIP).

Table 14: Some Error Conditions in Operation of 4600 Series IP Telephones

Condition		Cause/Resolution
The telephone continually reboots, or reboots continuously about every 15 minutes.		**CAUSE:** The telephone cannot find the call server. **RESOLUTION:** Ensure that MCIPADD is administered either manually or through DHCP, TFTP, or HTTP, as appropriate. **CAUSE:** This might be a firmware fault because the MAC address in memory is corrupted. **RESOLUTION:** Return the telephone to Avaya for repair.
The message light on the telephone turns on and off intermittently, but the telephone never registers.		**CAUSE:** This is a hardware fault. **RESOLUTION:** The telephone must be returned to Avaya for repair.
The telephone stops working in the middle of a call,	**AND** no lights are lit on the telephone and the display is not lit.	**CAUSE:** Loss of power. **RESOLUTION:** Check the connections between the telephone, the power supply, and the power jack. For example, verify that either static addressing was not used or that any changes to static addresses were entered correctly.
	AND power to the telephone is fine (and the telephone might have gone through the restarting sequence).	**CAUSE:** Loss of path to Avaya Media Server, DHCP Lease expired, or DHCP server not available when telephone attempts to renegotiate DHCP lease. **RESOLUTION:** As above. Note that if the telephone is attached to a 30A switched hub, upon loss of Ethernet connectivity, the usual `No Ethernet` message is not displayed.

1 of 6

Table 14: Some Error Conditions in Operation of 4600 Series IP Telephones (continued)

Condition		Cause/Resolution
The telephone was working, but does not work now,	**AND** no lights are lit on the telephone and the display is not lit.	**CAUSE:** Loss of power. **RESOLUTION:** Check the connections between the telephone, the power supply, and the power jack.
	AND power to the telephone is fine, but there is no dial tone. The display might show "System Busy."	**CAUSE:** Loss of communication with the PBX switch. **RESOLUTION:** Check LAN continuity from the PBX to the telephone using ARP or trace-route and from the telephone to the PBX by invoking a Feature button. Verify that LAN administration has not changed for the Gatekeeper, TN 2302AP circuit packs, or the LAN equipment (routers, servers, etc.) between the switch and the telephone. Verify no one changed the telephone settings locally using the **VIEW** and **ADDR** codes, as described in the *4600 Series IP Telephone Installation Guide*. Verify the telephone volume is set high enough. Finally, conduct a self-test.
	AND the telephone was recently moved.	**CAUSE:** Loss of communication with the PBX. **RESOLUTION:** As above, but pay particular attention to the possibility that the telephone is being routed to a different DHCP server, or even a different PBX switch. If so, the new server or switch might need to be administered to support the telephone.
	AND the network was recently changed to upgrade or replace servers, re-administer the Avaya Media Server, add or change NAT, etc.	**CAUSE:** Loss of communication with the PBX. **RESOLUTION:** As above.

Table 14: Some Error Conditions in Operation of 4600 Series IP Telephones (continued)

Condition	Cause/Resolution
The telephone works, but the audio quality is poor, specifically:	
the user hears echo when speaking on a handset.	**CAUSE:** Echo from digital-to-analog conversion on your Avaya Media Server trunk. **RESOLUTION:** Verify which trunk is causing the echo, and swap the trunk's Trunk Termination parameter on the PBX.
the user hears echo on a headset, but not on a handset.	**CAUSE:** Improper headset adapter. **RESOLUTION:** Replace adapter with Avaya's M12LU or 3412-HIC adapters. We recommend the M12LU, since it supports Automatic Gain Control.
the user is on Speaker and hears no echo, but the far-end hears echo.	**CAUSE:** Room acoustics. **RESOLUTION:** Ensure that there are six inches or so of blank space to the right of the telephone. If that is insufficient, use the handset.
the user experiences sudden silences such as gaps in speech, or static, clipped or garbled speech, etc.	**CAUSE:** Jitter, delay, dropped packets, etc. **RESOLUTION:** One or more Quality of Service (QoS) features should be implemented in the network. See Chapter 3 of the *4600 Series IP Telephone Installation Guide*. **CAUSE:** Improper non-Category 5 wiring. **RESOLUTION:** Replace non-Category 5 wiring with Category 5 wiring.
The 4612 or 4624 IP Telephone works properly except the telephone does not ring.	**CAUSE:** The Ringer Off (**RngOF**) softkey feature has been activated. **RESOLUTION:** Use the softkey **Menu** option to access the **RngOF** feature. A downward-pointing triangle means the Ringer is off. Ensure that the triangle points up. Also, check the Volume setting on the telephone. Finally, do a self-test on the telephone.

3 of 6

Table 14: Some Error Conditions in Operation of 4600 Series IP Telephones (continued)

Condition	Cause/Resolution
The telephone works properly except for the Speaker.	**CAUSE:** The Speaker was turned off on the PBX (H.323 telephones) or the 46xxsettings file's SPEAKERSTAT parameter is set to "0" (SIP telephones). **RESOLUTION:** Administer the PBX to allow that station's Speaker to operate (H.323 telephones) or change the SPEAKERSTAT parameter value (SIP telephones). If that does not work, do a Self-test on the telephone, as explained in the *4600 Series IP Telephone Installation Guide*.
The telephone works properly, except incoming DTMF tones are not received.	**CAUSE:** The TN2302AP circuit pack does not pass in-band DTMF tones. **RESOLUTION:** None; the board is operating as designed.
The telephone works properly, except sidetone DTMF is not heard.	**CAUSE:** PBX suppresses sidetone DTMF. **RESOLUTION:** On PBX administration, on the Change-System-Parameters screen, enable On-Hook Dialing. If the user has Hands-Free Answer (HFA), answers a call using the Speaker and switches to the handset, pressing dialpad buttons does not send DTMF tones. This is a known bug, and the only current resolution is to disable HFA.
Hands-Free Answer (HFA) is administered but the telephone did not automatically answer a call.	**CAUSE:** HFA only works if the telephone is idle. A second call is ignored if it comes in while a call is in progress, including ringing before the first call is answered. **RESOLUTION:** None.
The TFTP application terminates and asks for registration.	**CAUSE:** Non-Avaya shareware or freeware TFTP applications often cease operating to request registration. **RESOLUTION:** *Short-term:* Restart the application. *Long-term:* Register the product or replace it with an application that does not behave this way, for example, Avaya's TFTP application.
The TFTP or HTTP script file and settings file are ignored (not being used by the telephone).	**CAUSE:** The system value AUTH is set to 1 (HTTPS required) but no valid address is specified in TLSSRVR. **RESOLUTION:** Change AUTH to 0 (zero), or enter a valid address for TLSSRVR.

4 of 6

Table 14: Some Error Conditions in Operation of 4600 Series IP Telephones (continued)

Condition		Cause/Resolution
The TFTP or HTTP script file is ignored or not used by the telephone,	**AND** the TFTP or HTTP server is a LINUX or UNIX system.	**CAUSE:** The telephone expects lines of the script file to terminate with a **<Carriage Return> <Line Feed>**. Some UNIX applications only terminate lines with **<Line Feed>**. Editing the script file with a UNIX-based editor can strip **<Carriage Return>**s from the file. Doing so causes the entire file to be treated as a comment, and thus be ignored. **RESOLUTION:** Edit the script file with a Windows®-based editor, or another editor that does not strip out the **<Carriage Return>**. **CAUSE:** UNIX and LINUX systems use case-sensitive addressing and file labels. **RESOLUTION:** Verify the file names and path in the script file are accurately specified.
	AND telephone administration recently changed.	**CAUSE:** The ***46xxupgrade.scr*** file was edited incorrectly, renamed, etc. **RESOLUTION:** Download a clean copy of the ***46xxupgrade.scr*** file from the Avaya support Web site, and do not edit or rename it. Customize or change *only* the ***46xxsettings*** file, as discussed in Chapter 4: Server Administration.
Telephone power is interrupted while the telephone is saving the application file **and** the TFTP or HTTP application stops responding.		**CAUSE:** The TFTP or HTTP server stops responding if power is interrupted while a telephone is saving the application file. **RESOLUTION:** Restart the TFTP or HTTP server, as applicable.
The DHCP server indicates the 4600 Series IP Telephone reports itself as a Token Ring device, and refuses to provide the telephone an address.		**CAUSE:** Early versions of the 4600 Series IP Telephones erroneously report being a Token Ring device. With most DHCP servers, this does not matter. Some LINUX servers, however, refuse to issue addresses to Ethernet devices reporting to be Token Ring devices. **RESOLUTION:** Administer the DHCP server to delete all MAC and IP Addresses associated with Lucent Technologies or Avaya, or allow the associated DHCP leases to expire.
Telephone does not register with Avaya Communication Manager.		**CAUSE:** Use of IP telephone firmware R2.3 and greater requires TN799C V3 or greater. **RESOLUTION:** Upgrade TN circuit packs to TN799C V3 or greater.

5 of 6

Table 14: Some Error Conditions in Operation of 4600 Series IP Telephones (continued)

Condition		Cause/Resolution
The user indicates a 4610SW/4620/4620SW/ 4621SW/4622SW/4625SW-specific or 4630/4630SW-specific application is not accessible.		**CAUSE:** The ***46xxsettings*** script file is not pointed to accurately, or is not properly administered to allow the application. **RESOLUTION:** Assuming the user is meant to have that application, verify the 46xxsettings script file is properly specified for your system, including case if your file server is UNIX or LINUX, and extension. Then, verify all the relevant parameters indicated in Table 11 and Table 12, are accurately specified in the 46xxsettings file.
The user indicates a 4610SW/ 4620SW/4621SW/ 4622SW/ 4625SW-specific or 4630/ 4630SW-specific application is not accessible,	**AND** the script file is on a TFTP server and the telephone is a SIP telephone.	**CAUSE:** SIP telephones only obtain script files, application files, and 46xxsettings files from HTTP servers. **RESOLUTION:** Move the relevant files to an HTTP server, and administer the HTTPSRVR parameter accordingly.
On-hook dialing cannot be performed, Speed Dial labels and administered feature buttons are not available, and only one call appearance can be accessed.		**CAUSE:** Unnamed registration is enabled and the user did not provide an extension and password at the **Extension** prompt. **RESOLUTION:** Instruct the user to enter the extension and password. Alternately, disable unnamed registration.
PHY2STAT was set using the INT local procedure as specified in the *4600 Series IP Telephone Installation Guide*,	**BUT** the 4610SW, 4620/4620SW, 4621SW, 4622SW, 4625SW uses the original setting instead of using the new setting following a reboot.	**CAUSE:** The telephone's FTP Backup/Restore feature is enabled. The user specified a setting file for the **PC Ethernet Interface** setting through the Options menu. The user-specified setting is overriding the Local Procedure PHY2STAT setting. **RESOLUTION:** Use the Options menu to change the setting to the value you want, so the INT local procedure is not necessary. Alternatively, use the Options menu to change the **PC Ethernet Interface** setting to **Auto-negotiation**. Then make all future changes using the INT local procedure.

6 of 6

There are three areas where installers can troubleshoot problems before seeking assistance from the system or LAN administrator:

1. Check the power and Ethernet wiring to ensure that:
   - all components are plugged in correctly.
   - there is LAN connectivity in both directions to all servers - DHCP, TFTP, HTTP, call server. Note that if the telephone is attached to a 30A switched hub, upon loss of Ethernet connectivity the usual `No Ethernet` message is not displayed.
   - if the telephone is supposed to be powered from the LAN, ensure that the LAN is properly administered and is compliant with IEEE 802.3af-2003.
2. If you are using static addressing:
   - use the **`VIEW`** command to find the names of the files being used and verify that these filenames match those on the file server. Check on the Avaya Web site to verify whether the correct files are being used. Note that the 4601 IP Telephone does not support static addressing and therefore, does not support the **`VIEW`** command.
   - use the **`ADDR`** option to verify IP Addresses.
   - use the **`QoS`** option to verify QoS parameters.

     See Chapter 3 of the *4600 Series IP Telephone Installation Guide*.
3. If the 4600 Series IP Telephone is not communicating with the DHCP, TFTP, HTTP, or media server, make a note of the last message displayed. Consult the system administrator.

The Clear Administrative Option

Sometimes, you might want to remove *all* administered values, user-specified data, and option settings, etc. Essentially, you want to return a telephone to its initial “clean slate” condition. Usually, this is done to pass a telephone to a new, dedicated user when the user’s L O G O F F option is not sufficient. For example, if the new user has the same extension, but has different permissions than the previous user. The C L E A R option erases all administered data such as:

- static programming,
- file server and call server programming, and
- user settings, including Speed Dial button labels and locally programmed Feature button labels.

C L E A R then restores all such data to default values. The C L E A R option does not affect the software load itself, so if you have upgraded the telephone, the telephone retains the latest software. Once a telephone is Cleared, you can administer it normally.

CAUTION:

This procedure erases all administered data, without any possibility of recovering the data.

Note:

Only telephones with Release 2.1 or later software support the CLEAR Administrative Option.

Use the following procedure to clear the telephone of its administrative, user-assigned and options values.

1. While the telephone is on-hook and idle, press the following sequence of keys on the faceplate of the telephone:

   Mute 2 5 3 2 7 # (Mute C L E A R #)

   Note:

   Press the **Mute** button momentarily. Do not press this button while pressing other keys/buttons. The 4630/4630SW IP Telephones and the 4690 IP Conference Telephone do not have a dedicated **Hold** button. For all other 4600 Series IP Telephones, pressing the **Hold** button instead of the **Mute** button also works.

   The following text displays left-justified at the top of the display:

   ```
   Clear all values?
   *=no    #=yes
   ```

2. If you do not want to clear all values, press ***** (no) to terminate the procedure and retain the current values.

   A screen displays the following prompt on the top line:

   ```
   Are you sure?
   *=no    #=yes
   ```

3. Press the ***** button to terminate the procedure without clearing the values. Press the # button to clear all values to their initial default values.

   A confirmation tone sounds. If the telephone already has an IP Address that was obtained through DHCP, the telephone transmits a DHCPRELEASE message. The following text displays left-justified at the top of the display:

   ```
   Clearing values.
   ```

   The telephone is cleared to its “out of the box” state.

The Reset Administrative Option

As indicated in some troubleshooting procedures, sometimes it is appropriate to reset the 4600 Series IP Telephone. Procedures on how to do so are printed in this section. You can also find reset procedures in Chapter 3 of the *4600 Series IP Telephone Installation Guide*. These parameters and settings are reset to default values, including “null” as applicable, when the Reset procedure finishes:

- Registration extension and password.
- All values administered by local procedures, in accordance with Chapter 3 of the *4600 Series IP Telephone Installation Guide*.
- All values previously downloaded using DHCP or from a TFTP settings file. These values, of course, are usually restored when the telephone re-registers after the reset.

Note:

If **PROCSTAT** was administered to **1**, as described in Chapter 4: Server Administration, you cannot invoke the **R E S E T** option. In addition, if **PROCPSWD** was administered as non null, you must enter that value after you press **Mute** and before you press **R E S E T**.

Reset System Values

Use the following procedure to reset all system initialization values to the application software default values.

CAUTION:

This procedure erases all static information, without any possibility of recovering the data.

1. While the telephone is on-hook and idle, press the following sequence of keys on the faceplate of the telephone:

   Mute 7 3 7 3 8 # (Mute R E S E T #)

   Note:

   Press the **Mute** button momentarily. Do not press this button while pressing other keys/buttons. The 4630/4630SW IP Telephones and the 4690 IP Conference Telephone do not have a dedicated **Hold** button. For all other 4600 Series IP Telephones, pressing the **Hold** button instead of the **Mute** button also works.

The 4601 IP Telephone flashes both Message Waiting indicators 500 milliseconds on, 500 milliseconds off to indicate user input is expected. All other IP telephones display the following text left-justified at the top of the display:

```
Reset values?
*=no    #=yes
```

CAUTION:

All static information is erased without any possibility of recovering the data as soon as you press the # button.

2. If you do not want to reset the system values, press ***** (no) and proceed to Step 4.

   Pressing the pound sign (#) to reset the system values on a 4601 IP Telephone produces a confirmation tone. The 4601's Message Waiting indicators illuminate but do not flash to indicate no entry is allowed while the system values are being reset. All other phones display a screen with the following prompt on the top line:

```
Are you sure?
*=no    #=yes
```

3. Press the ***** button to continue without resetting the values and proceed to Step 4. Or, press the # button to reset values to their defaults.

   If the telephone already has an IP Address that was obtained through DHCP, the telephone transmits a DHCPRELEASE message. All phones except the 4601 display the following text left-justified at the top of the display while the system values are reset to defaults:

```
Resetting
values.
```

   The telephone resets from the beginning of registration, which takes a few minutes.

4. If you do not reset the telephone, all IP telephones except the 4601 display the following prompt:

```
Restart phone?
*=no    #=yes
```

5. Press the ***** key to terminate the procedure without restarting the telephone. Otherwise, press # and follow the next procedure to restart the telephone.

Restart the Telephone

Use the following procedure to restart the telephone.

1. While the telephone is on-hook and idle, press the following sequence of keys on the faceplate of the telephone:

   Mute 7 3 7 3 8 # (Mute R E S E T #)

   Note:

   Press the **Mute** button momentarily. Do not press this button while pressing other keys/buttons. The 4630/4630SW IP Telephones and the 4690 IP Conference Telephone do not have a dedicated **Hold** button. For all other 4600 Series IP Telephones, pressing the **Hold** button instead of the **Mute** button also works.

   The 4601 IP Telephone flashes both Message Waiting Indicators 500 milliseconds on, 500 milliseconds off to indicate user input is expected. All other IP telephones display the following text left-justified at the top of the display:

   ```
   Reset values?
   *=no    #=yes
   ```

2. Press the # button to reset values to their defaults, or ***** to continue a restart without resetting the values to their defaults.

   Pressing the pound sign (#) to reset the system values on a 4601 IP Telephone produces a confirmation tone. The 4601's Message Waiting indicators illuminate but do not flash to indicate no entry is allowed while the system values are being reset. All other phones display the following text left-justified at the top of the display while the system values are reset to defaults:

   ```
   Resetting
   values.
   ```

   Once the system values are reset, the following prompt displays on all IP telephones, except the 4601:

   ```
   Restart phone?
   *=no    #=yes
   ```

3. Press the ***** key to terminate the procedure without restarting the telephone.

   Press the # key to restart the telephone.

   The remainder of the procedure depends on the status of the boot and application files. See Appendix A of the *4600 Series IP Telephone Installation Guide*.

The View Administration Option

If you are using static addressing and encounter problems, use this procedure to verify the current values of system parameters and file versions.

Note:

Also use the **ADDR** option to view IP Addresses covered in “Static Addressing Installation” in Chapter 3 of *4600 Series IP Telephone Installation Guide*. IP Addresses might have been entered incorrectly*. Verify whether you were provided with correct IP Addresses.*

If **PROCPSWD** is administered as indicated in Chapter 4: Server Administration, you must type the Local Procedure password after pressing **Mute**, and before pressing **V I E W**.

The 4601and 4601+ IP Telephone do not support static addressing, and therefore do not support the V I E W command.

1. While the telephone is on-hook and idle, press the following sequence of keys on the faceplate of the telephone:

   Mute 8 4 3 9 # (Mute V I E W #)

   Note:

   Press the **Mute** button momentarily. Do not press this key while pressing other keys. The 4630 IP Telephone does not have a dedicated **Hold** button. For all other 4600 Series IP Telephones, pressing the **Hold** button instead of the **Mute** button also works.

   The following text displays left-justified at the top of the display:

   ```
   View settings
   *=next   #=exit
   ```

2. Press the ***** button at any time during viewing to display the next name and system value pair from Table 15. The first pair displays again after the last pair displays.

   Press the # button at any time during viewing to terminate the procedure and restore the user interface to its previous state.

   The names and values display in the order shown in Table 15.

Table 15: Viewing Parameter Values

Name	System Value	Format
Model	***46ccDccc***	Up to 8 ASCII characters: Model.
Phone SN	***ccccccccccccc ccccccccc***	Telephone Serial Number, up to 18 ASCII characters (which display on both lines).
PWB SN	***ccccccccccccc ccccccccc***	Printed Wiring Board (circuit board) Serial Number, up to 18 ASCII characters (which display on both lines). Applies to all telephones with a display except 4602, 4602SW, 4602SW+, and 4610SW.
PWB comcode	***nnnnnnnnn***	9 ASCII numeric characters: PWBCC. Applies to all telephones with a display, except 4602, 4602SW, and 4610SW.
PWB version	***ccccccccc***	9 ASCII numeric characters. Applies only to the 4602, 4602SW, 4602SW+, and 4610SW.
MAC address	***hh:hh:hh:hh:hh:hh***	Each octet of the MAC address displays as a pair of hexadecimal numbers.
L2 tagging	***ccccccccc***	Up to 9 ASCII characters: “on” if NVL2Q = 1 “off” if NVL2Q = 2 “auto: on” if NVL2Q = 0 and 802.1Q tagging is on, and “auto: off” if NVL2Q = 0 and 802.1Q tagging is off.
VLAN ID	***cccc***	Up to 4 ASCII characters: L2QVLAN if 802.1Q tagging is on and “none” if 802.1Q tagging is off.
IP Address	***nnn.nnn.nnn.nnn***	Up to 15 ASCII characters: IPADD.
Subnet mask	***nnn.nnn.nnn.nnn***	Up to 15 ASCII characters: NETMASK.
Router	***nnn.nnn.nnn.nnn***	Up to 15 ASCII characters: the IP Address of the router in use.

1 of 3

Table 15: Viewing Parameter Values (continued)

Name	System Value	Format
File server	***nnn.nnn.nnn.nnn.nnnnn***	Up to 21 ASCII characters: the IP Address and port of last file server used successfully during initialization (“0.0.0.0” if no HTTP or TFTP file server was used successfully).
Call server	***nnn.nnn.nnn.nnn.nnnnn***	Up to 21 ASCII characters: IP Address and port of call server currently in use, if any, otherwise “0.0.0.0”.
802.1X	***pass-thru mode***	If system parameter DOT1X = 0
	pass-thru with Logoff	If system parameter DOT1X = 1
	Supplicant mode	If system parameter DOT1X = 2
Group	***nnn***	Up to 3 ASCII numeric characters: GROUP.
Protocol	***cccccccc***	Up to 8 ASCII characters, depending on the system-specific signaling protocol (H.323, SIP, etc.) currently being used.
	filename.ext	Up to 16 ASCII characters: name of the application code file (“big app”) currently stored in the telephone.
	ccccccc Ethernet	Ethernet connection. From 2 to 7 ASCII characters, either “100Mbps,” “10 Mbps,” or “No.”
	filename.ext	Up to 16 ASCII characters. Name of the boot code file (“little app”) currently stored in the telephone.
	ccccccccccc	Up to 10 ASCII characters. DSP code version.
	ccccccccccc	Up to 10 ASCII characters. DSP hardware version, displayed only if a DSP hardware version identifier is available.
Build	***ccccccccccc***	Build identifier. Up to 10 ASCII characters.

2 of 3

Table 15: Viewing Parameter Values (continued)

Name	System Value	Format
DHCPSTD		DHCP standard flag. If “1,” the telephone strictly follows the DHCP standard by giving up IP Addresses when the DHCP lease expires. If “0,” the telephone uses the IP Address until it detects reset or a conflict
Audio environment		Audio environment selection index (0 to 107); the AUDIOENV system value.
Handset sidetone		The AUDIOSTHS system value where 0=No change, 1=6dB below nominal, 2=no sidetone - infinite loss.
Headset sidetone		The AUDIOSTHD system value where 0=No change, 1=6dB below nominal, 2=no sidetone - infinite loss.

3 of 3

Error Messages

The 4600 Series IP Telephones issue messages in English only. The IP telephones also display messages from the switch, which outside the United States might issue messages in the local language.

Note:

Because the 4601 IP Telephone does not have a display, it is limited in its ability to provide visual feedback and error messages. Nonetheless, some feedback is available and presented as applicable. For more information, see Table 18: Possible Error Messages During 4601 IP Telephone Installation or Operation on page 145.

Table 16: Possible Error Messages During Installation or Operation of 4600 Series IP Telephones

Error Message	Cause/Resolution
During Installation	
`Bad Router`	**CAUSE:** The telephone cannot find a router based on the information in the DHCP file for GIPADD. **RESOLUTION:** Change administration on DHCP, as indicated in DHCP in Chapter 4: Server Administration.
`Checksum error`	**CAUSE:** Downloaded application file was not downloaded or saved correctly. **RESOLUTION:** The telephone automatically resets and attempts to re-initialize.
`DHCP: CONFLICT` `* to program`	**CAUSE:** At least one of the IP Address offered by the DHCP server conflicts with another address. **RESOLUTION:** Review DHCP server administration to identify duplicate IP Address(es).
`Discover` ***`aaa.bbb.ccc.ddd`***	**CAUSE:** The 46xx telephone is attempting to discover (and register with) the Gatekeeper at IP Address *aaa.bbb.ccc.ddd*. **RESOLUTION:** If this message appears for more than a few seconds, especially if the IP Address keeps changing, the telephone is unable to contact the Gatekeeper. Verify network connectivity between the telephone and the Gatekeeper, or revise the Gatekeeper addresses in the DHCP/script files to point to different Gatekeepers. See Administering 4600 Series IP Telephones on Avaya Media Servers (H.323 Only), DHCP, TFTP (H.323 Only), and HTTP.
`Discovering...`	**CAUSE:** The telephone is seeking a gatekeeper on the media server, using its administered gatekeeper list. **RESOLUTION:** Wait for a valid registration to occur, or press # to interrupt the search and re-initialize manual or DHCP/script files procedures.
`File too large` `Cannot save file`	**CAUSE:** The telephone does not have sufficient room to store the downloaded file. **RESOLUTION:** Verify the proper filename is administered in the script file, and that the proper application file is located in the appropriate location on the file server.

1 of 6

Table 16: Possible Error Messages During Installation or Operation of 4600 Series IP Telephones (continued)

Error Message	Cause/Resolution
`Gateway Error`	**CAUSE:** DEFINITY Release 8.4 does not have an H.323 station extension for this telephone. **RESOLUTION:** On the station administration screen, ensure the DCP set being aliased for this IP telephone has an H.323 station extension administered, in accordance with switch administration instructions.
`Hardware failure`	**CAUSE:** Hardware failure prevented downloading of application file. **RESOLUTION:** Replace telephone.
`IP Address in use by another`	**CAUSE:** The telephone has detected an IP Address conflict. **RESOLUTION:** Verify administration to identify duplicate IP Address(es).
`NAPT Error`	**CAUSE:** A device between the telephone and the call server is invoking Network Address Port Translation, which the 4600 Series IP Telephones do not support. **RESOLUTION:** Remove or re-administer the NAPT device or move the telephone.
`No Ethernet`	**CAUSE:** When first plugged in, the IP telephone is unable to communicate with the Ethernet. **RESOLUTION:** Verify the connection to the Ethernet jack, verify the jack is Category 5, etc. Note that if the telephone is attached to a 30A switched hub, upon loss of Ethernet connectivity, the usual “No Ethernet” message is not displayed.
`No file server address`	**CAUSE:** The file server IP Address in the IP telephone’s memory is all zeroes. **RESOLUTION:** Depending on the specific requirements of your network, this may not be an error. If appropriate, either administer the DHCP server with the proper address of the file server, or administer the telephone locally using the ADDR option. The *4600 Series IP Telephone Installation Guide* explains the ADDR option.
`No Socket`	**CAUSE:** The telephone has registered with the call server, but network problems have prevented the telephone from opening a TCP socket. **Note:** This message only occurs on older software versions. Telephones with newer software automatically reset. **RESOLUTION:** Investigate the network problem normally.

2 of 6

Table 16: Possible Error Messages During Installation or Operation of 4600 Series IP Telephones (continued)

Error Message	Cause/Resolution
`System busy`	**CAUSE:** Most likely, the number of IP endpoints on the Avaya Media Server is already at maximum, Less likely, network resource is unavailable. **RESOLUTION:** The telephone was attempting to access a network resource (DHCP server, TFTP server, or the Avaya Media Server) and was not successful. Check the resource being called upon for its availability. If the resource appears operational and properly linked to the network, verify addressing is accurate and a communication path exists in both directions between the telephone and the resource.
`System Error`	**CAUSE:** The Avaya Media Server has an unspecified problem. **RESOLUTION:** Consult your Avaya Media Server administration and troubleshooting documentation.
During Registration	
`Bad Router`	**CAUSE:** The telephone cannot find a router based on the information in the DHCP file for GIPADD. **RESOLUTION:** Change administration on DHCP, as indicated in DHCP in Chapter 4: Server Administration.
`Extension error`	**CAUSE:** An invalid Avaya Media Server Registration extension has been entered. **RESOLUTION:** Reenter the extension if entered incorrectly. If appropriate, verify proper extension with respect to switch administration.
`Extension in use`	**CAUSE:** The specified extension is already in use, according to the Avaya Media Server. **RESOLUTION:** You will be told if the telephone using the same extension is on a call or not. Regardless, you can proceed to take over the extension or to login using a different extension. Telephones with large displays, such as the 4610SW or 4625SW, and Release 2.7 software provide detailed messages and specially labeled softkeys to guide you through either alternative. If the telephone has a two-line display, or does not support Release 2.7, you can either press the # key twice to take over the extension and log the other telephone off or you can press #, then ***** to enter a different extension.

3 of 6

Table 16: Possible Error Messages During Installation or Operation of 4600 Series IP Telephones (continued)

Error Message	Cause/Resolution
`Failed to set phone IP Address`	**CAUSE:** The 4600 Series Telephone was originally installed on one switch with Static Addressing, and has subsequently been installed on another switch with an active DHCP server assigning dynamic IP Addresses. **RESOLUTION:** Reset the telephone.
`Incompatible`	**CAUSE:** This release of the Avaya Media Server does not support the current version of the IP telephone. **RESOLUTION:** Upgrade to the current version of Avaya Media Server software.
`IP Address Error`	**CAUSE:** The gatekeeper reports an invalid IP Address. **RESOLUTION:** This should never happen. Contact Avaya.
`Message light blinks on and off, and the telephone did not complete registration`	**CAUSE:** The telephone has a hardware fault. **RESOLUTION:** Replace the telephone.
`NAPT Error`	**CAUSE:** A device between the telephone and the call server is invoking Network Address Port Translation, which the 4600 Series IP Telephones do not support. **RESOLUTION:** Contact the System Administrator to remove or re-administer the NAPT device.
`No Call Server Address - Resetting`	**CAUSE:** The system parameter MCIPADD does not contain at least one non-zero IP Address or DNS Name, causing the telephone to reset. **RESOLUTION:** Add the IP Address(es) using static addressing (manual telephone setting), updating the settings file, or normally through DHCP administration.
`No Proxy Found` (SIP only)	**CAUSE:** A problem with the list of SIP registration/proxy servers. **RESOLUTION:** Review the server administration to ensure that the correct addresses are specified. Verify the proper operation of the Registration Server(s) and the intervening network.
`No Socket`	**CAUSE:** The telephone has registered with the call server, but network problems have prevented the telephone from opening a TCP socket. **Note:** This message only occurs on older software versions. Telephones with newer software automatically reset. **RESOLUTION:** Press the # button to reset the telephone and contact the [Network] System Administrator to report the network problem.

4 of 6

Table 16: Possible Error Messages During Installation or Operation of 4600 Series IP Telephones (continued)

Error Message	Cause/Resolution
`Password Error`	**CAUSE:** An invalid PBX Registration password has been entered. **RESOLUTION:** Re-enter the password if entered incorrectly. If appropriate, verify proper password with respect to switch administration.
`Registering...` (SIP only)	**CAUSE:** It is normal for this message to occasionally appear for a short time. If the message appears for an extended time period, the telephone is unable to register. **RESOLUTION:** Verify proper operation of the Registration Server(s) and the intervening network.
`Registration Failed` (SIP only)	**CAUSE:** The registration process failed. **RESOLUTION:** Verify the proper operation/administration of the Registration Server(s) and the intervening network.
`Resource Error`	**CAUSE:** The Avaya Media Server rejects the registration request. **RESOLUTION:** Verify your Avaya Media Server administration to ensure the telephone's proper IP Address, extension, and password are being used.
`Timeout Error`	**CAUSE:** Protocol timeout error. **RESOLUTION:** Retry. If failure continues, check network congestion, addresses, etc. to identify cause of timeout.
`Unauthorized` (SIP only)	**CAUSE:** The Registration Server does not recognize the extension and password. **RESOLUTION:** Reenter the correct extension and password. If the problem persists, contact the System Administrator.
`Undefined Error`	**CAUSE:** An error has occurred without an identifiable cause. **RESOLUTION:** Conduct self-test, restart the telephone, and if no other cause becomes evident, replace the telephone.
`Wrong Set Type`	**CAUSE:** The Avaya Media Server does not recognize the set type. **RESOLUTION:** Ensure that the Avaya Media Server is properly administered to expect the appropriate telephones for the IP Address and extension.

5 of 6

Table 16: Possible Error Messages During Installation or Operation of 4600 Series IP Telephones (continued)

Error Message	Cause/Resolution
During Operation	
`Discover aaa.bbb.ccc.ddd`	**CAUSE:** The 46xx telephone is attempting to discover (and register with) the Gatekeeper at IP Address *aaa.bbb.ccc.ddd*. **RESOLUTION:** If this message appears for more than a few seconds, especially if the IP Address keeps changing, the telephone is unable to contact the Gatekeeper. Verify network connectivity between the telephone and the Gatekeeper, or revise the Gatekeeper addresses in the DHCP/script files to point to different Gatekeepers. See Administering 4600 Series IP Telephones on Avaya Media Servers (H.323 Only), DHCP, TFTP (H.323 Only), and HTTP.
`Discovering...`	**CAUSE:** The user is on a call when the network connection between the telephone and call server is interrupted, but the call stays connected. The telephone automatically starts procedures to register with the call server again. However, until registration succeeds, the user has no access to Avaya Communication Manager features and functionality. This message alerts users to the lack of connection to the call server. **RESOLUTION:** This is the same message, with the same implications and Resolution as the Discovering... message on page 139.
`Current options and Speed Dial entries have not yet been backed up`	**CAUSE:** An attempt to save the current options and Speed Dial entries on the FTP server has not yet been made or is in progress. **RESOLUTION:** Wait for a message stating that backup was successful.
`The FTP Server Name is not known. Please check the FTP Server IP Address`	**CAUSE:** Invalid or missing server name. **RESOLUTION:** Verify the FTPSRVR address is the file server to which backup data should be saved. Verify that the FTPDIR value is the correct directory path for that file server.
`The FTP Server has not yet responded, so backup has not yet succeeded`	**CAUSE:** The FTP server has not responded to the attempt to backup/restore. **RESOLUTION:** Try again, verify the FTP server address, verify the FTP server is online, and/or verify the network connectivity.

6 of 6

Table 17: Possible Error Messages During 4610SW, 4620/4620SW, 4621SW, 4622SW, 4625SW, and 4630/4630SW Backup/Restore

Error Message	Cause/Resolution
`The FTP Server has denied access Please check FTP Setup parameters`	**CAUSE:** The FTP server has reported that it did not store data. **RESOLUTION:** Verify the FTP server setup parameters, as indicated on the FTP Setup Parameters screen. See “FTP Setup” in Chapter 8 of the *4630/4630SW IP Telephone User Guide, or* see “Backup/Restore Options” in Chapter 6 of the appropriate User Guide for the telephone type.
`The FTP Server was unable to store the backup file`	**CAUSE:** The FTP server has reported that it could not store the data. **RESOLUTION:** Verify administration and available capacity/ filespace on the FTP server.

Troubleshooting the 4601 IP Telephone

This section describes specific problems that can occur during 4601 IP Telephone installation, administration or normal operation, and possible ways of resolving these problems.

In Table 18, the Error Messages shown in the first column correspond to the equivalent conditions described in “Chapter 4" of the *4600 Series IP Telephone Installation Guide* and Table 16: Possible Error Messages During Installation or Operation of 4600 Series IP Telephones. However, rather than displaying messages, the 4601 turns its LEDs on and off to indicate an error condition, as described in Table 18’s second column. In addition, not all error conditions result in unique LED indications.

Table 18: Possible Error Messages During 4601 IP Telephone Installation or Operation

Error Message	4601 Visual Indication/Cause/Resolution
`Extension Error`	**VISUAL INDICATION:** Message Waiting indicators at top of telephone and the left middle of the faceplate display a broken flutter for a total of 5 cycles (with one cycle being alternating 50 milliseconds on, 50 milliseconds off for 500 milliseconds followed by 500 milliseconds off). **CAUSE:** The PBX does not recognize the extension entered or cannot find a valid gatekeeper. **RESOLUTION:** Confirm the extension is correct and is correctly administered on the switch. Then try registration again, taking particular care to enter the extension accurately.

1 of 3

Table 18: Possible Error Messages During 4601 IP Telephone Installation or Operation (continued)

Error Message	4601 Visual Indication/Cause/Resolution
`Extension in Use`	**VISUAL INDICATION:** If the extension is being used, the 4601 attempts registration. The first attempt causes the Message Waiting indicators at the top of telephone and left middle of the faceplate to display a broken flutter. The broken flutter alternates 50 milliseconds on, 50 milliseconds off for 500 milliseconds, followed by 500 milliseconds off five times. Then the indicators flash continuously, awaiting user entry. Then the 4601 makes a second registration attempt using the *same* extension. This attempt causes the Message Waiting indicators at the top of telephone and left middle of the faceplate to display a continuous broken flutter. The broken flutter alternates 50 milliseconds on, 50 milliseconds off for 500 milliseconds followed by 500 milliseconds off. In addition, Call Appearance Line b's LED flashes continuously until either the "*" or "#" button is pressed. **CAUSE:** The PBX detects an extension conflict with an existing set or Softphone. **RESOLUTION:** You can force the current telephone to register, and thereby disconnect the other user, by pressing #. The 4600 Series IP Telephone prompts you again for the extension and password. If you enter the same extension and password, you must confirm that you want to unregister the original user. Press # to unregister the original user and register the current telephone. Then press ***** to reset the telephone and enter a different extension and password. If you take no action within 20 minutes, the telephone attempts registration again, repeating the process until either you intervene or power is lost.
`IP Address in use by another`	**VISUAL INDICATION:** All LEDs are steadily lit, except Call Appearance Line A, which is flashing. **CAUSE:** The telephone has detected an IP Address conflict. **RESOLUTION:** DHCP restart is automatically initiated. No user action required.
`No Ethernet`	**VISUAL INDICATION:** No LEDs flash when telephone is plugged in. **CAUSE:** Telephone is unable to communicate with the Ethernet. **RESOLUTION:** Verify the connection to the Ethernet jack, verify the jack is Category 5, verify power is applied on the LAN to that jack, etc.
`Password Error`	**VISUAL INDICATION:** Message Waiting indicators at top of telephone and left middle of faceplate display a broken flutter for a total of 5 cycles (with one cycle being alternating 50 milliseconds on, 50 milliseconds off for 500 milliseconds followed by 500 milliseconds off), then flash continuously, awaiting user entry. **CAUSE:** The PBX does not recognize the password entered. **RESOLUTION:** Confirm the password is correct, then try registration again, taking particular care to enter the password accurately.

2 of 3

Table 18: Possible Error Messages During 4601 IP Telephone Installation or Operation (continued)

Error Message	4601 Visual Indication/Cause/Resolution
`System busy`	**VISUAL INDICATION:** Message Waiting indicators at top of telephone and left middle of faceplate display a broken flutter continuously (alternating 50 milliseconds on, 50 milliseconds off for 500 milliseconds followed by 500 milliseconds off) until either the "*****" or "**#**" button is pressed. **CAUSE:** Most likely, the number of IP endpoints on the PBX is already at maximum, Less likely, network resource is unavailable. **RESOLUTION:** The telephone was attempting to access the PBX and was not successful. Check the resource being called upon for availability. If the resource appears operational and properly linked to the network, verify addressing is accurate and that a two-way telephone/resource communication path exists. Press ***** to retry the process with the same values, or # to restart and enter the extension and password again.
`System Error`	**VISUAL INDICATION:** Message Waiting indicators at top of telephone and left middle of faceplate display a broken flutter continuously (alternating 50 milliseconds on, 50 milliseconds off for 500 milliseconds followed by 500 milliseconds off) until either the "*****" or "**#**" button is pressed. **CAUSE:** The PBX has an unspecified problem. **RESOLUTION:** Press ***** to retry the process using the same values or # to restart and re-enter the extension and password. Consult your Avaya Media Server administration and troubleshooting documentation.
`Undefined Error`	**VISUAL INDICATION:** Message Waiting indicators at top of telephone and left middle of faceplate display a broken flutter continuously (alternating 50 milliseconds on, 50 milliseconds off for 500 milliseconds followed by 500 milliseconds off) until either the "*****" or "**#**" button is pressed. **CAUSE:** The PBX has rejected registration for an unspecified reason. **RESOLUTION:** Press ***** to retry the process using the same values or # to restart and re-enter the extension and password. Consult your Avaya Media Server administration and troubleshooting documentation.
`Wrong Set Type`	**VISUAL INDICATION:** Message Waiting indicators at top of telephone and left middle of faceplate display a broken flutter continuously (alternating 50 milliseconds on, 50 milliseconds off for 500 milliseconds followed by 500 milliseconds off) until either the "*****" or "**#**" button is pressed. **CAUSE:** The PBX does not recognize the set type. **RESOLUTION:** Ensure the PBX is properly administered to expect the appropriate telephone for the IP Address and extension. Press ***** to retry the process using the same values or # to restart and re-enter the extension and password.

3 of 3

Appendix A: Avaya - 46xx IP Telephone MIB

Downloading the Avaya - 46xx IP Telephone MIB

The custom Management Information Base (MIB) is available in ***.txt*** format for free download at http://www.avaya.com/support. Follow these links:

- Under **Technical Database**, select **Telephone Devices & User Agents**.
- Then under **IP Telephones and User Agents**, select **4600 IP Telephones**.
- Then select **Programming and Administration**.

Note:

All 4600 Series IP Telephones of a given Release have the same MIB, regardless of whether they are SIP or H.323 telephones.

Appendix B: Creating Web Sites for the 4630/4630SW IP Telephone

Introduction

This appendix describes the capabilities and limitations of the 4630/4630SW IP Telephone's Web Browser. We also provide suggestions to help you design Web sites for viewing on the 4630/4630SW. This appendix is intended for 4630/4630SW IP Telephone Web Browser [Web page] designers, and assumes readers are familiar with HTML, Style Sheets, and ECMAScript.

This appendix serves two primary functions:

- To present technologies implemented in the 4630/4630SW IP Telephone's Web Access application, including any limitations or non-standard implementations, and
- To provide a suggested model for developing effective Web pages for Web browser viewing.

This appendix is not intended to provide technical details on setting up a Web server, nor does it provide information on Web server technologies. Finally, this document is not intended to provide an introduction to Web browser protocols or technologies.

Note:

See the Avaya Web site for a link to sites where HTML templates are available for customizing.

Any subsequent reference to the 4630 IP Telephone in this appendix applies equally to the 4630SW IP Telephone.

General Background

The 4630 IP Telephone display is a 1/4-VGA (320 pixels wide by 240 pixels high, 256 colors supported) display.

The data types and other features supported in the browser include:

- HTML 4.01
- Cascading Style Sheets (CSS), Levels 1 and 2
- Document Object Model (DOM) Level 1
- Images: GIF and JPEG
- ECMAScript (JavaScript) 1.4
- HTTP 1.0 and 1.1
- Secure Sockets Layer (SSL) 2.0 and 3.0
- Cookies stored in non-volatile memory
- Click-to-Dial Functionality

Browser Features and Behavior

This section presents technologies implemented in the 4630 IP Telephone Web Access application, along with any limitations or non-standard implementations. Style sheets are now the preferred mechanism to control Web page appearance and have made most attribute specifications with tags obsolete. Therefore, the majority of tag attributes were not tried. The attributes that were tested were those of real interest to specific tags. The browser is HTML 4.0 compliant, with a few minor differences as noted where appropriate.

Note:

The sections in this appendix show comments specific to the 4630 IP Telephone and its browser in italics.

Document Skeleton

Certain tags define the basic framework of an HTML document. Most browsers are usually good at dealing with missing tags. However, when you apply style sheets it is essential that you follow the tag structures. Even ignoring style sheets, it is considered good style to follow the HTML rules. The following tags make up the basic skeleton of an HTML document:

- <html> indicates the start of an HTML document.
- <head> indicates the start of an HTML document's header. Title, meta definitions, ECMAScript function definition, document level style sheet definition, and external style sheet inclusion are all done in the header section.
- <title> sets the title of the document. This is usually shown in the frame of the browser window. *On the telephone, the title is shown in the Top Line Information Display Area.*
- <body> indicates the start of the body of an HTML document. The rest of the document is embedded between the start and end <body> tags.
- <meta> adds additional information about an HTML page. *Web walking tools usually use this tag, which is of little use in browsers, and has no effect on the telephone*.

Content-Based Style

Content-based tags deal with identifying words, phrases or chunks of text, or images as having a specific meaning or context. The intent of content-based tags is not to show physically marked text. However, it is not wrong for a browser to show content-based text in a distinct style, such as font style.

Each content-based tag is shown with a brief description, and any physical effects imposed by the browser.

- <abbr> indicates an abbreviation.
  Using this tag has no effect.
- <address> indicates an address.
  Using this tag has no effect.
- <acronym> indicates an acronym.
  The enclosed text is shown in an italic font.
- <cite> indicates a bibliographic citation or reference.
  The enclosed text is shown in an italic font.
- <code> indicates source code of a program.
  The enclosed text is shown in a monospaced font.
- <del> indicates deleted text. It shows editorial markup.
  A line is drawn through enclosed text.

- <dfn> indicates a definition for a term. This is usually used with the first appearance of a term in a document.
  The enclosed text is shown in an italic font.
- indicates emphasis on a string of text. This is the contextual equivalent of using the <i> (italic) tag.
  The enclosed text is shown in an italic font.
- <ins> indicates inserted text. It shows editorial markup.
  The enclosed text is shown underlined.
- <kbd> indicates keyboard input. This is similar to the <code> tag, but with a different contextual intent.
  The enclosed text is shown in a monospaced font.
- <samp> indicates literal text.
  The enclosed text is shown in a monospaced font.
- indicates emphasis on some text, but in a stronger contextual sense than the tag. This is the contextual equivalent of using the <b> (bold) tag.
  The enclosed text is shown in a bold font.
- <var> indicates source code variables. This is similar to the <code> tag, but with a different contextual intent.
  The enclosed text is shown in an italic font.

Logical Style

Tags that control logical style provide a similar functionality to those that control content-based style, but they have no implicit visual characteristics or contextual meaning. Instead, they only provide a means of invoking a style sheet. These tags, like all others, might have an ID and class attribute set. Using style sheet rules for these class names and IDs allows the designer to provide decoration, font, and color styles for each section. Thus, these tags can be considered to be designer-defined, content-based tags:

- indicates a division. A newline is inserted between the previous text and the text following the tag. No physical changes are noticeable, except those implemented in style sheets.
- indicates a spanned section of text is placed immediately after the text that precedes the tag with a newline. No physical changes are noticeable, except those implemented in style sheets.

Physical Style

Physical tags are effectively the opposite of content-based tags. The text in a physical tag might have no meaning whatsoever, outside what the designer intended. These tags show text in a distinct style. Physical tags usually affect font style. Each physical style tag is shown with a brief description and any physical effects the browser imposes.

- <b> indicates that the text appears in a bold font weight.
- <big> indicates that the text appears one point size larger than the current text.
- <i> indicates that the text appears in an italic font.
- <small> indicates that the text appears one point size smaller than the current text.
- <sub> indicates that the text appears as a subscript to the current text. The text is shown one point size smaller.
- <sup> indicates that the text appears as a superscript to the current text. The text is shown one point size smaller.
- <tt> indicates that the text appears as teletype text. The text is shown in a monospaced typeface font.

Physical Spacing and Layout

Physical spacing and layout tags define the basic structure of a document. Headings, paragraphs, tables and lists all provide some basic physical and logical layout to a page. Each spacing and layout tag is shown with a brief description, and any unusual behavior is described.

- <p> indicates the start of a new paragraph. A blank line is inserted between previous text and text following the <p> tag.
-
 indicates to insert a breakpoint. A newline is inserted between previous text and text following the <br> tag.
- <pre> indicates no formatting rules apply to the text that follows. This implies that no wrapping will be applied to this text, which can result in adding a horizontal scrollbar to view the text.
- <hr> indicates that a newline and a horizontal rule line should be inserted between the previous text and text following the <hr> tag.
- <blockquote> indicates that the following text is a quote, and should be offset in some way. The embedded text is shown with newlines before and after the text, with spacing to the left and right. Within that “block” of text, normal wrapping rules apply.
- <q> indicates that the following text is a short quote, and should be shown in double-quotes (according to documentation). This text appears as normal text, with no physical identifying indications.
- <h1> - <h6> indicate heading sections. Each level is one point smaller than the previous level, with <h1> being the largest.

The section titled Maintaining Context on page 163 contains design guidelines for maintaining user context.

Lists and Tables

For presentation of data in a logical format, lists and tables are two of the more important sets of tags. Since space is at a premium in the browser, tables should be used with discretion. While they provide sets of text, which are easy for the eye to process, they can quickly become cumbersome if misused in this browser. Both width and height are limited, so the data provided in the table cells should be short pieces of text. Beyond that, the page designer should come up with a different model for presenting the data, possibly using lists and divisions.

Lists

- starts an ordered list. Provides a list with some type of numbering: upper-case letters, lower-case letters, digits, upper-case roman numerals, lower-case roman numerals. Setting the type attribute is ignored in the browser.
- starts an unordered list. Provides a list with bullets to the left of each item.
- adds an item to an ordered or unordered list.
- <dl> starts a definition list. Provides a list with two fields per list item. The first is a term and the second is the term's definition.
- <dt> adds a new definition term to a definition list.
- <dd> adds a new term definition to a definition list.

Tables

The new HTML 4.0 table tags, <thead>, <tbody> and <tfoot> are all implemented. These tags allow printed pages to have headers and footers when the table is longer than a single page. Since the 4630 IP Telephone Web Browser has no print capability, we recommend that these tags not be used.

- <table> starts a table layout.
- <caption> adds a caption to a table. The align attribute allows a caption to be placed above or below the table. This attribute has no effect in the telephone.
- <tr> adds a new table row to a table.
- <th> adds a header for some column(s) of a table.
- <td> adds a piece of data for some row(s) and column(s) of a table.
- <thead> defines a set of table header rows. The intent of this tag is to provide a set of header rows for each printed page. While viewing the page in a browser, the header has no more effect than the <th> tag. What it provides for the designer is a more logical breakout of the data. The table’s header area is easily recognizable, since it appears between the <thead> start and end tags.
- <tbody> defines the main body of a table, when used with the <thead> and <tfoot> tags.

- <tfoot> defines a footer for a table. This tag can contain multiple rows. Like the <thead> tag, the intent of this tag is to provide a set of footer rows for each printed page. Viewing the page in a browser has no additional effect. And like the <thead> tag, this tag provides a logical breakout of the data for the designer.
- <colgroup> defines a column group. It can be used as a single definition of identical columns or as a container for dissimilar columns. The span attribute defines what columns are parts of each group.
- <col> controls the appearance of one or more columns within a column group.

Images

The 4630 IP Telephone Web Browser handles both GIF and JPEG image formats. No other image formats, included animated GIFs, are supported. Note that images take up a large amount of memory compared to text and that updating the display can be an issue. For these reasons, we recommend keeping images to a minimum.

The image tags that can be used on the browser are:

- <img> displays an image.
- <map> display a client-side image. Client-side images have shaped regions called areas. These areas are tied to URLs or ECMAScript functions. Clicking on an area in a region executes the ECMAScript function.
- <area> defines an area in a <map> image. Each area uses the href attribute to define a URL to jump to, or an ECMAScript to execute when that area is clicked.

See the Design Guidelines on page 161 for information on displaying images.

Links

As of Release 1.8, the 4630/4630SW IP Telephones support dialing from hyperlinks. To dial from a link, a given link's href attribute value must of the form **tel:*nnnnn*** or javascript:dial('***nnnnn***'). Selecting that link passes the characters ***nnnnn*** to the 4630/4630SW Phone application for direct dialing.

Hyperlinks are the heart of the Web browser's power. The link allows the user to:

- click text or an image to jump to another Web site,
- click text or an image to jump to another page within this site, or
- click text or an image to jump to another area on a page.

Although URLs allow you to use various protocols, use only HTTP and HTTPS for the 4630 IP Telephone Web Browser.

- <a> specifies the full or relative URL for a hyperlink. When using the target attribute, never use the _blank name. With the exception of frames, the 4630 IP Telephone Web Browser is not intended to be a multi-window browser. Thus, if a page attempts to reference a new, non-frame window, the browser becomes confused and a reboot is necessary.
- <base> defines the default target to be used in all <a> tags. This is done by setting the target attribute of the <base> tag. If the target attribute is set in the <a> tag, the <base> tag value is ignored.

Using the target attribute with the Web Access Application is strongly discouraged because the application supports a single window for browsing. The use of the target attribute can cause the browser software to create a new window that is outside the Web Access Application's control.

Frames

Frames allow multiple windows to be created on the browser's base window. The browser is effectively split up into multiple areas. Each frame can be given a name or ID. Using the target attribute of the <a> tag, a Web page can be displayed in another frame.

Although frames behave as defined, the small size of the screen makes them impractical to use. Just like tables, frames take up too much room on the display. One can, though, take advantage of frames by having a small “table of contents” frame with images for links. In general, however, use of frames is strongly discouraged.

- <frameset> defines an area for a set of frames.
- <frame> defines a single frame in a frameset.
- <iframe> defines an in-line frame.
- <noframes> provides a fallback for browsers that don't handle frames. If the designer intends to use frames and make these pages available to the telephone, this tag should certainly be employed.

See the Design Guidelines on page 161 for information on displaying frames.

Forms

HTML forms provide the user the ability to enter data into a Web browser. This data can then be passed to the Web server for processing. It is difficult to predict what Web designers might have in mind for the 4630 IP Telephone Web Browser. However, all forms-related tags have been verified, and the results are presented here.

- <form> defines the basic input form, and defines the action to be performed when the **Submit** button is selected, through the action attribute.

- <input> defines most user input. The type of attribute defines the type of input to use. The <button> tag was created to replace type values of button, reset and submit, in a cleaner, more flexible way. Other type values available are checkbox, hidden, image, password, radio, and text. The type value file is useless in this browser's context, since this control's intent is to allow the user to select a file on their local disk.
- <button> defines a button that the user can select. This tag behaves much like the <input type=button> tag, except the physical appearance is three-dimensional. Also, the button can display any text, image, or combination thereof.
- <fieldset> encapsulates a section of a form's contents to create a group of related form controls. The telephone browser puts a simple box around the fieldset.
- <label> associates a relationship between a form control and one or more text labels. Labels can be tied to form controls by the form attribute in the label and the id attribute in the form control. They can also be tied by embedding the form control inside the <label> tag, for example, <label>Name: <input type=text id=name></label>.
- <legend> gives a label to a <fieldset> tag. This label appears at the top of the fieldset section of the form, with a line separating the legend from the rest of the fieldset.
- <optgroup> provides nested, cascading menus to the user. This does not seem to work.
- <option> defines the values available in a <select> scrolling list or drop-down menu.
- <select> defines scrolling lists and drop-down menus.
- <textarea> provides free-form user input and display. This provides a scrolled text area for the user to read or type text.

Character Entities

As with any syntactic language, HTML has certain characters that have special meaning. The two most obvious characters are the < and > symbols, which surround all tags. These characters cannot be typed in directly if the designer's intent is to display these characters. Thus, all characters that a Web browser can display are assigned numeric values. In addition, many of these characters also are assigned names. The numeric values are entered into the source Web page as ***&#nnn*;** where ***nnn*** is some 3 digit value. For example, the < symbol is entered as '<'. Name values are entered into the source Web page as &name; where name is the name associated with this character. Again, using the < symbol, this would be entered as '<'. The browser fully supports the set of characters defined by the World Wide Web Consortium, in conformance with the standard.

Colors

The browser supports 256 colors. Colors can be specified by name, RGB percentages, or RGB raw numbers. The HTML and CSS specifications suggest 16 named colors.

The 4630 IP Telephone Web Browser recognizes these color names, which are:

- aqua
- black
- blue
- fuchsia
- gray
- green
- lime
- maroon
- navy
- purple
- red
- silver
- teal
- olive
- white
- yellow

Beyond these 16 well-known names, we recommend using RGB percentages or raw numbers to specify colors.

Fonts

Font specifications are one of the most important styles you can apply to a Web browser. Because of the 4630 IP Telephone's screen size, the browser has only a single font available for use. Font weights such as normal and bold are supported. Finer font values, such as lighter and bolder are not supported. Normal and Italic font styles are also supported. Font sizes are also supported, specified by either percentages or raw numbers. However, percentages below 50% all appear as the same size.

Although we found some problems with font specifications, fonts behave reasonably well given the screen's size and resolution. The only major problem found is the inability to specify font families.

See the Design Guidelines on page 161 for information on displaying images.

Cookies

Cookies can be a useful feature in maintaining the state of a user when interacting with a Web site. HTTP provides no state information, such as when or how often a user visits a site. Cookies allow Web sites to track this information by storing a simple set of values on the browser for the current session. Usually, browsers also provide the ability to save cookies to disk, to retain this information between sessions. However, the 4630 IP Telephone Web Browser has no such ability to save any data between sessions. Cookies do behave well within the realm of the current session, and can be used if desired. The 4630 IP Telephone has a maximum of 8Kilobytes of data available for cookie storage.

Design Guidelines

This section presents guidelines for developing a good model that effectively presents Web pages for 4630 IP Telephone Web Browser viewing. The biggest challenge in designing pages for this browser is the limited amount of space available for viewing the pages. The 4630 IP Telephone screen is a 1/4-VGA display. Part of that screen is lost to the browser by the 4630 IP Telephone's main controls. Page layout must be effective and efficient, to avoid causing more lost space through additional screen controls like scrollbars. Font sizing can make or break a page's usability. You must find a balance between fitting as much text as is possible, and allowing users to read the text without straining their eyes.

Fixed-Width Objects

One of a Web browser's primary functions is to present text wrapped at the browser window's right border. When dealing with internationalization, text would wrap at the left border. The browser always attempts to avoid adding a horizontal scrollbar. However, if you use fixed-width objects, like tables and pre-formatted (<pre> tag) text, wrapping becomes secondary to presenting the data exactly as HTML dictates.

Web browsers do not resize themselves larger when you add scrollbars. Thus, if there are more lines of text than can fit in the browser window's height, a vertical scrollbar is added. This now takes up some of the width of the browser, and less text displays on a single line. If text is wider than the browser's width, a horizontal scrollbar is added. This now takes up some of the browser's height, and fewer lines of text are displayed.

Given the small size of the browser, it is highly desirable to avoid causing scrollbars to appear. Unless the amount of text shown in a page is kept to a bare minimum, avoiding a vertical scrollbar is unlikely. However, avoiding fixed-width objects, or ensuring that the size of fixed-width is kept small, gains some viewable space. If scrolling is a requirement, vertical scrolling is usually better perceived by users than horizontal scrolling.

Images

Using images in a Web page is always a concern. For example, a page with many images can slow up downloading. While this is still a concern in the telephone, an image's size has a much greater effect. Browser and telephone memory is limited. Each image can use a sizable amount of memory, overwhelming the browser. Use an image only if it is essential to a page.

Images also fall into the realm of fixed-width objects. Check all images to verify that they do not cause a horizontal scrollbar to be added. Scale down a browser image by setting the width and height attributes of the <img> tag. Or instead, scale the images when setting up the Web site. Scaling images during Web site setup avoids forcing the browser to deal with the sizing. Using the width and height attributes scales the image after it is downloaded by the browser. Scaling

images during setup also speeds up image downloading. Finally, reducing the size of the image reduces the amount of memory used.

Animated GIF images are a bad idea since they use up quite a bit of memory. Additionally, because of the persistence of the LCD screen, animated images tend to smear in the browser and lose their effectiveness. Therefore, animated GIFs are considered “not supported” with this telephone.

Frames

While contents and document text frames provide a useful method to browse a series of pages, frames also use up real estate, just like scrollbars. Even if the frame decorations are all turned off, a frame containing the majority of the document text suffers the problems discussed in Images—the frame width is smaller, increasing the chances of adding a horizontal scrollbar. Additionally, a single text line has fewer viewable characters, and the page becomes even more difficult to read and comprehend. Using simple top and bottom page or section navigation buttons, can make up for the missing contents frame.

The interaction between frames and scrollbars is another important area of concern. While most browsers manage scrolling within each frame independently, the 4630 Web Access Application only scrolls the entire (single) window. Scrolling by window moves the user's view of the frames as a whole, but does not scroll any of the data in individual frames. Data is likely to be in frames that can never be seen.

Minimal screen real estate and scrolling issues make frames something to avoid.

Fonts

Font size is a major concern in the browser. Without designer intervention, the browser displays text as if it were running on a PC in a normal width and height display. This means that the fonts shown appear huge relative to the screen size. As a result, only seven lines of text can be viewed in the browser when no font sizing is applied. Additionally, only about 25 characters are viewable per line. From a practical point of view, this situation is not usable.

To make the browser usable, perform some form of font sizing to allow a reasonable amount of text to be viewed per screen. Ideally, put font sizing in a single external style sheet, and make all pages reference this style sheet. Do not set font sizes in document-level style sheets, or even worse, for in-line style sheets or <font> tags. Doing so makes it very difficult for the designer to update font changes, and runs the risk of failing to make a universal change. Use a single external style sheet to manage consistency in the pages.

Define fonts using a static external style sheet. You can also generate a style sheet dynamically using some form of server-side application, such as a CGI script or a Java servlet. Dynamic style sheet generation allows the server to decide, per user, what font size to use. This in turn allows the user to notify the server to change the font size. All HTML pages would have an external style sheet reference, another server-side executable. This executable dynamically

generates font information based on the cookie, form component, or configuration value, relative to the IP Address of the telephone. Using a static external style sheet makes page development and testing much easier, since it appears the same way to both the designer and the reader. Allowing the user to choose a font size forces more work on the designer to verify that all fixed size items appear acceptably

Maintaining Context

Given the small screen area, a user can become easily lost. Headings are often not in view, and the user, if distracted by other work, can lose a sense of context. Style sheets can help maintain this sense of context through color. The and tags are intended to provide page designer-defined content-based style. By defining classes of tags with various colors and border styles, the designer provides additional information. However, a significant number of people suffer from some form of color blindness. Thus, it may be necessary to design pages both with and without using color styles.

User Interaction

As these design guidelines indicate, HTML forms work reasonably well in the Browser. However, due to telephone limitations as an input device, keyboard input can be difficult. A complete keyboard is made available based on the context of mouse selection. When a text input control is on-screen, the user just clicks the input control. The keyboard appears, with the browser thrown into a small scrolling area. The input control is roughly centered in the scrolling area. The user can then press the software keys and the text is shown in the input control. Simply pressing the **Done** button dismisses the keyboard, and the input control shows the newly typed text. While this interaction technically works fine, it can be difficult to type a large amount of text from a user perspective. So avoid user input unless it is absolutely necessary. When necessary, keep user input to a minimum.

Click-to-Dial Functionality

Embedded as **<a href="javascript:dial('nnnn')">** ***nnnn*** is passed to the Phone application to initiate a telephone call.

Example:

```
<html><head>
<body>
<table border="0" width="100%">
     <tr>
     <td>
          <b>Call IT Technical Support:</b><br>
          <a href="javascript:dial('1-555-555-5151')">
          <img border="0" src="call.gif">1-555-555-5151
          </a>
     </td>
     <tr>
     <td>
          <b>Call Bill Pay:</b><br>
          <a href="javascript:dial('1-555-555-5152')">
          <img border="0" src="call.gif">1-555-555-5152
          </a>
     <td>
     <tr>
</table>
</body></html>
```

The generated code is rendered as this Web page:

Appendix C: Creating Web Sites for Other 4600 Series IP Telephones

Introduction

A Web browser is available for Web application development in these 4600 Series IP H.323 Telephones:

- 4610SW
- 4620/4620SW
- 4621SW
- 4622SW
- 4625SW

You can also develop Web applications for these SIP IP Telephones:

- 4610SW
- 4620SW/4621SW

See the *4600 Series IP Telephones Application Programmer Interface (API) Guide*, available on the Avaya support Web site (http://www.avaya.com/support) for detailed information about Web browser requirements, characteristics, and functionality. That guide also provides suggestions to help design Web sites for viewing on applicable IP telephones.

Appendix D: Administering Thin Client Directories

Introduction

If you have a corporate database that supports the Lightweight Directory Access Protocol (LDAP), Avaya's Thin Client Directory application can communicate with that database. IP telephone users can then use their phones to search for names, telephone numbers, or other information. Using search results, users can call a person directly, store a number on a Speed Dial button, and view more details about the person.

The Thin Client Directory application applies only to these IP telephone types:

- 4610SW
- 4620/4620SW
- 4621SW
- 4622SW
- 4625SW

See the *4600 Series IP Telephones Application Programmer Interface (API) Guide*, available on the Avaya support Web site (http://www.avaya.com/support) for detailed information about installing and administering Avaya's Thin Client Directory application.

Appendix E: The Push Feature

Introduction

Release 2.1 of the 4600 Series IP Telephones provided support for a feature called “Push,” which applies to the 4610SW, 4620, and 4620SW Telephones. Release 2.2 introduced additional IP Telephones, the 4621SW, the 4622SW, and the 4625SW, to which the Push feature also applies. In all cases, the Push feature applies only to telephones supporting H.323, and not to SIP IP telephones.

Push gives the System Administrator the capability to use WML protocol to:

- send *content* to a telephone without first receiving a user request, and
- potentially override what the user is otherwise experiencing.

You can send pushed content to a single telephone, a group of phones, or the entire enterprise.

Push Content

Three types of content can be pushed, with one of two types of priorities, normal and barge-in. The content types are:

- **Text Messages** on the top display line. If a pushed text message has barge-in priority, the message overwrites whatever else is currently displayed. However, other subsequent messages can, in turn, overwrite the pushed message. If the pushed text message has normal priority, it is buffered in the telephone and displayed when no higher priority message is being displayed. Up to 56 characters can be pushed to the top line in a given message.
- **WML Web pages** can be pushed to the telephone’s WML browser. If a pushed Web page has barge-in priority, the content overwrites whatever else is currently displayed to the user.

  If the push of a Web page has normal priority, the Web page does not override what the user sees. If the user has the Web application displayed, normal-priority pushed content overrides what is otherwise displayed. If the Web application is not being displayed, normal-priority pushed content loads in the background. When the user invokes the Web application, the pushed content displays, subject to certain restrictions. For this reason, you might want to accompany a Web push with a corresponding pushed text message, alerting users there is Web content to view.

- **Audio Messages** (RTP) can be pushed. Pushed audio messages can drive the telephone off-hook, if necessary and play the pushed message through the telephone's Speaker. If the audio push has barge-in priority, the audio message is presented to the user, even if the user is on a call. In this latter case, the far-end is automatically placed on Hold and does not hear the pushed audio message.

A given push can include any or all of the three content forms, but can have only one priority. You can optionally accompany each push with notification tones to draw the user's attention to the telephone and to the pushed content.

Push Priorities

Barge-in pushes, as the name implies, are meant for information important to get to the user. An example of a barge-in push might be an audio message alerting users that the building is closing because of inclement weather. You can accompany that message with a Web page detailing weather conditions. There are very few circumstances that can prevent barge-in pushes from being presented to the user. Of course, network conditions can prevent actual delivery of the pushed content.

Use normal pushes for less-essential or less time-critical information. An example might be "Mary has birthday cake in her office." A normal push might or might not be presented to the user. For example, a normal audio push is not presented to a user already on a call. Or, a normal text message would not display until a higher priority message completes.

For More Information on Push

The specifications and interactions of pushed content are beyond the scope of this document. The *4600 Series IP Telephones Application Programmer Interface (API) Guide* provides detailed information about developing Push content and administering the Push feature. Find the API on the Avaya support Web site, http://www.avaya.com/support. Further information, including sample applications, is also available in a Software Developer Toolkit on the Avaya support Web site.

For more detailed assistance in developing applications, also visit the Solutions Directory on Avaya's Developer Connect Web page (www.devconnectprogram.com) and follow the *Find a Solution* link. The Directory has a list of companies you can work with to develop applications. The Solutions Directory lists all current Developer Connection Program Members, with whom you can work to develop applications, and their innovative solutions. The members in this directory have all been approved in the program and are compliance-tested to assure customer satisfaction.

Appendix F: Sample Upgrade Script File

Introduction

Each software release provides an updated script file, a sample of which is shown below. The filenames following the **SET APPNAME** command in this sample are examples only and may not match those used in production.

```
Release Date:  July 25, 2006
#
# H323-Centric 46XX Software Upgrade Script
# Additions for 460xP
#
# This file upgrades the following telephones to the
# indicated releases:
#     4601  - GA Release 2.3
#     4601+ - GA Release 2.3
#     4602D, 4602SW H.323 - GA Release 2.3
#     4602+  - GA Release 2.3
#     4602D, 4602SW SIP - GA Release 2.2.2
#     4602SW+ SIP - GA Release 2.3
#     4606, 4612, 4624 - GA Release 1.8.3
#     4610SW, 4620SW, 4621SW, 4622SW H.323 - GA Release 2.4
#     4620 H.323 - GA Release 2.3
#     4610SW, 4620SW, 4621SW SIP - GA Release 2.2.2
#     4625  - GA Release 2.5
#     4690  - GA Release 2.0
#
# *This script file will load multi-byte software
#  with support for English, Chinese, Japanese and
#  Cyrillic display fonts into ACP 4610SW, 4620SW,
#  4621SW, and 4622SW Telephones
```

```
#
#
################################################
# BOOTAPP VERSION NUMBERS
#   46xx: 83
#   4601: 2.3
#   4601+: 2.3
#   4602: 2.3
#   4602+: 2.3
#   4602/02SW SIP: 2.3
#   4602SW+ SIP: 2.3
#   4610: 2.4
#   4620: 2.3
#   4620SW: 2.4
#   4621SW: 2.4
#   4622SW: 2.4
#   4625SW: 2.5
#   4690: 2.0
################################################
################################################
# BIGAPP VERSION NUMBERS
#   46xx: 1.8.3
#   4601: 2.3
#   4601+: 2.3
#   4602: 2.3
#   4602+: 2.3
#   4602/02SW SIP: 2.2.2
#   4602SW+ SIP: 2.3
#   4610: 2.4
#   4610 SIP: 2.2.2
#   4620: 2.3
#   4620SW: 2.4
```

```
#   4620SW SIP: 2.2.2
#   4621SW: 2.4
#   4621SW SIP: 2.2.2
#   4622SW: 2.3
#   4625SW: 2.5
#   4690: 2.0
################################################

#check bootApp version

IF $MODEL4 SEQ 4601 goto BOOTAPP4601
IF $MODEL4 SEQ 4602 goto BOOTAPP4602
IF $MODEL4 SEQ 4606 goto BOOTAPP46XX
IF $MODEL4 SEQ 4610 goto BOOTAPP4610
IF $MODEL4 SEQ 4612 goto BOOTAPP46XX
IF $MODEL4 SEQ 4620 goto BOOTAPP4620
IF $MODEL4 SEQ 4621 goto BOOTAPP4620
IF $MODEL4 SEQ 4622 goto BOOTAPP4620
IF $MODEL4 SEQ 4624 goto BOOTAPP46XX
IF $MODEL4 SEQ 4625 goto BOOTAPP4625
IF $MODEL4 SEQ 4690 goto BOOTAPP4690

goto END

# BOOTAPP4601
IF $MODEL  SEQ 4601D01A goto BOOTAPP4601D
IF $MODEL  SEQ 4601D01B goto BOOTAPP4601P
goto END

# BOOTAPP4601D
IF $BOOTNAME SEQ 4601dbte1_82.bin goto CONVERT01
IF $BOOTNAME SEQ cvt01_2_3.bin goto AVAYACODE01
```

```
IF $BOOTNAME SEQ b01d01b2_3.bin goto DEF46XX
IF $APPNAME  SEQ a01d01b2_3.bin goto END
goto GET01_182
goto END

# GET01_182
SET APPNAME 4601dbte1_82.bin
goto END

# CONVERT01
SET APPNAME cvt01_2_3.bin
goto END

# AVAYACODE01
SET APPNAME b01d01b2_3.bin
goto END

# BOOTAPP4601P
IF $BOOTNAME SEQ b01d01p2_3.bin goto DEF46XX
SET APPNAME b01d01p2_3.bin
goto END

# BOOTAPP4602
IF $MODEL  SEQ 4602D01A goto BOOTAPP4602D
IF $MODEL  SEQ 4602D02A goto BOOTAPP4602SW
IF $MODEL  SEQ 4602D02B goto BOOTAPP4602P
goto END

# BOOTAPP4602D
IF $BOOTNAME SEQ 4602dbte1_82.bin goto CONVERT02
IF $BOOTNAME SEQ cvt02_2_3.bin goto AVAYACODE02
IF $BOOTNAME SEQ b02d01b2_3.bin goto DEF46XX
```

```
IF $APPNAME  SEQ a02d01b2_3.bin goto END
goto GET02_182
goto END

# GET02_182
SET APPNAME 4602dbte1_82.bin
goto END

# CONVERT02
SET APPNAME cvt02_2_3.bin
goto END

# BOOTAPP4602SW
IF $BOOTNAME SEQ 4602sbte1_82.bin goto CONVERT02SW
IF $BOOTNAME SEQ cvt02sw_2_3.bin goto AVAYACODE02
IF $BOOTNAME SEQ b02d01b2_3.bin goto DEF46XX
IF $APPNAME  SEQ a02d01b2_3.bin goto END
goto GET02S_182
goto END

# GET02S_182
SET APPNAME 4602sbte1_82.bin
goto END

# AVAYACODE02
SET APPNAME b02d01b2_3.bin
goto END

# CONVERT02SW
SET APPNAME cvt02sw_2_3.bin
goto END
```

```
# BOOTAPP4602P
IF $BOOTNAME SEQ b02d02p2_3.bin goto DEF46XX
SET APPNAME b02d02p2_3.bin
goto END

# BOOTAPP4620
IF $MODEL SEQ 4620D01A goto BOOTAPP4620A
IF $MODEL SEQ 4620D01B goto BOOTAPP4620B
IF $MODEL SEQ 4621D01A goto BOOTAPP4620B
IF $MODEL SEQ 4622D01A goto BOOTAPP4620B
goto END

# BOOTAPP4610
IF $BOOTNAME SEQ b10d01b2_4.bin goto DEF46XX
SET APPNAME b10d01b2_4.bin
goto END

# BOOTAPP4620A
IF $BOOTNAME SEQ b20d01a2_3.bin goto DEF46XX
SET APPNAME b20d01a2_3.bin
goto END

# BOOTAPP4620B
IF $BOOTNAME SEQ b20d01b2_4.bin goto DEF46XX
SET APPNAME b20d01b2_4.bin
goto END

# BOOTAPP4625
IF $BOOTNAME SEQ b25d01a2_5.bin goto DEF46XX
SET APPNAME b25d01a2_5.bin
goto END
```

```
# BOOTAPP4690
IF $BOOTNAME SEQ 4690_020005.bin goto DEF4690
SET APPNAME 4690_020005.bin
goto END


# BOOTAPP46XX
IF $BOOTNAME SEQ 46XXCOMMON.V83 goto DEF46XX
SET APPNAME bbla0_83.bin
goto END
################################
#  download  bigApp            #
################################
# DEF46xx
IF $MODEL4 SEQ 4601 goto DEF4601
IF $MODEL4 SEQ 4602 goto DEF4602
IF $MODEL4 SEQ 4606 goto DEF4606
IF $MODEL4 SEQ 4610 goto DEF4610
IF $MODEL4 SEQ 4612 goto DEF4624
IF $MODEL4 SEQ 4620 goto DEF4620
IF $MODEL4 SEQ 4621 goto DEF4620
IF $MODEL4 SEQ 4622 goto DEF4620
IF $MODEL4 SEQ 4624 goto DEF4624
IF $MODEL4 SEQ 4625 goto DEF4625

goto END

#bigApp for 4601 model
# DEF4601
IF $MODEL  SEQ 4601D01A goto DEF4601D
IF $MODEL  SEQ 4601D01B goto DEF4601P
goto END
```

```
# DEF4601D
SET APPNAME a01d01b2_3.bin
goto END

# DEF4601P
SET APPNAME a01d01p2_3.bin
goto END

#bigApp for 4602 and 4602SW SIP model
# DEF4602
IF $SIG SEQ 2 goto SIP_4602
IF $MODEL  SEQ 4602D01A goto DEF4602D
IF $MODEL  SEQ 4602D02A goto DEF4602SW
IF $MODEL  SEQ 4602D02B goto DEF4602P
goto END

#bigApp for 4602D model
# DEF4602D
SET APPNAME a02d01b2_3.bin
goto END

#bigApp for 4602SW model
# DEF4602SW
SET APPNAME a02d01b2_3.bin
goto END

# SIP_4602
#bigApp for 4602 SIP model
IF $MODEL  SEQ 4602D02B goto SIP_4602P
SET APPNAME s02d01b2_2_2.bin
goto END
```

```
# SIP_4602P
#bigApp for 4602+ model
SET APPNAME s02d02p2_2_3.bin
goto END

# DEF4602P
SET APPNAME a02d02p2_3.bin
goto END

#bigApp for 4606 model
# DEF4606
SET APPNAME def06r1_8_3.bin
goto END

# DEF4610
#bigApp for 4610 ACP model
IF $SIG SEQ 2 goto SIP_4610
SET APPNAME a10d01b2_4.bin
goto END

# SIP_4610
#bigApp for 4610 SIP model
SET APPNAME s10d01b2_2_2.bin
goto END


#bigApp for 4620 models
# DEF4620
IF $MODEL SEQ 4620D01A goto DEFAPP4620A
IF $MODEL SEQ 4620D01B goto DEFAPP4620B
IF $MODEL SEQ 4621D01A goto DEFAPP4620B
```

```
IF $MODEL SEQ 4622D01A goto H323_4620SW
goto END

# DEFAPP4620A
#bigApp for 4620 ACP model
SET APPNAME a20d01a2_3.bin
goto END

# DEFAPP4620B
IF $SIG SEQ 2 goto SIP_4620SW

# H323_4620SW
#bigApp for 4620SW ACP model
SET APPNAME a20d01b2_4.bin
goto END

# SIP_4620SW
#bigApp for 4620SW SIP model
SET APPNAME s20d01b2_2_2.bin
goto END

#bigApp for 4612 & 4624 model
# DEF4624
SET APPNAME def24r1_8_3.bin
goto END

#bigApp for 4625SW models
# DEF4625
SET APPNAME a25d01a2_5.bin
goto END

#bigApp for 4690 model
```

```
# DEF4690
#SET APPNAME XXXXXXXXXXXXXX.bin
goto END

# END
GET 46xxsettings.txt
```

Index

Numerical

4600 Series IP Telephones . . . 33
- Administering on Avaya Media Servers (H.323 Only) . . . 55
- Administering Options for . . . 96
- Administration Alternatives and Options . . . 52
- Creating Web Sites for . . . 167
- DHCP and File Servers . . . 34
- DNS Addressing . . . 107
- Initialization Process . . . 36
- Network Audio Quality Display . . . 83
- Restart . . . 134
- Scripts and Application Files . . . 74
- WAN Considerations . . . 35

4610SW, 4620/4620SW, 4621SW, 4622SW, and 4625SW IP Telephones
- Administering Thin Client Directories for . . . 169
- Application Status Flag (APPSTAT) . . . 119
- Backup/Restore . . . 121
- Customizable System Parameters . . . 116
- Customizing . . . 116

4630/4630SW IP Telephone
- Backup/Restore . . . 114
- Call Log Archive . . . 115
- Creating Web Sites for . . . 151
- Customizable System Parameters . . . 111
- customizing . . . 111

46xx IP Telephone MIB . . . 149
802.1X . . . 90

A

About This Guide . . . 9
Administering 4600 Series IP Telephones on Avaya Media Servers . . . 55
Administering DHCP and File Servers . . . 56
Administering H.323 and SIP IP Telephones on the Same Network . . . 54
Administering Options for the 4600 Series IP Telephones . . . 96
Administering the Thin Client Directories . . . 169
Administration Alternatives and Options for 4600 Series IP Telephones . . . 52
Application File and Upgrade Script, Choosing . . . 76
Application Files, and Scripts for 4600 Series IP Telephones . . . 74
Application Status Flag (APPSTAT) . . . 119
Application Status Flag (APPSTAT) for 4610SW, 4620/4620SW, 4621SW, 4622SW and 4625SW IP Telephones . . . 119
Applications . . . 41
Avaya - 46xx IP Telephone MIB . . . 149
Avaya Communication Manager Software Release 1.1 55
Avaya File Server Application . . . 72

B

Backup/Restore for 4610SW, 4620/4620SW, 4621SW, 4622SW and 4625SW IP Telephones . . . 121
Backup/Restore, for 4630/4630SW . . . 114

C

Call Log Archive, for 4630/4630SW . . . 115
Choosing the Right Application File and Upgrade Script File . . . 76
Clear Administrative Option . . . 130
Click-to-Dial Functionality . . . 164
Configuration and Installation, Suggestions for . . . 42
Conventions Used in This Guide . . . 17
Creating Web Sites for Other 4600 Series IP Telephones . . . 167
Creating Web Sites for the 4630/4630SW IP Telephone . . . 151
- Browser Features and Behavior . . . 152
- Click-to-Dial Functionality . . . 164
- Design Guidelines . . . 161
- General Background . . . 152

Customer Support . . . 25
Customizing
- 4610SW, 4620/4620SW, 4621SW, 4622SW and 4625SW IP Telephones . . . 116
- 4630/4630SW IP Telephone . . . 111
- Site-Specific Option Number (SSON) . . . 108
- System Parameters for 4610SW/4620/4620SW,4621SW, 4622SW, and 4625SW IP Telephones . . . 116
- System Parameters for 4630/4630SW IP Telephones . . . 112

D

Date and Time, Setting on SIP IP Telephones . . . 110
DEFINITY Releases 9, 9.5, and 10 . . . 55
Delay and Jitter . . . 28
DHCP and File Server Administration . . . 56
DHCP and File Servers . . . 34
DHCP and VoIP . . . 29

DHCP Configuration, Choosing 58
DHCP Generic Setup 59
DHCP Server 34
DHCP Server Setup 58
DHCP Server, Windows 2000 Setup 67
DHCP Server, Windows NT 4.0 Setup. 63
DHCP Software Alternatives 58
Dial Plan, Setting on SIP IP Telephones. 110
DNS Addressing 107
Document Change History 12
Document Organization 11

E

Enhanced Dialing Procedures 108
Enhanced Local Dialing 108
Error Conditions 123
Error Messages 138

F

File Server Application 72
File Servers 34
File Servers and DHCP Administration 56

G

GROUP System Value 79

H

H.323 and SIP, Administering on the same network . 54
Hardware Requirements 47
HTTP 30, 73
HTTP Generic Setup 73

I

IEEE 802.1X. 90
IETF Documents. 22
Initialization and Address Resolution 40
Initialization Process, for 4600 Series IP Telephones . 36
Installation and Configuration, Suggestions for. . . . 42
Installation, Network Information Required before installing 57
Intended Audience 10
IP Address Lists and Station Number Portability . . . 43
ISO/IEC, ANSI/IEEE Documents 25
ITU Documents 24

L

Link Layer Discovery Protocol (LLDP) 92
LLDP Data Units Transmitted 92

M

Media Server Field Names and Corresponding Script File Parameter Names 73
MIB, for 46XX IP Telephones 149

N

NAT 31
Network Assessment and VoIP 32
Network Audio Quality Display, on 4600 Series IP Telephones 83
Network Information
Required 56
Required Before Installation 57
Network Protocols 27
Network, Administering both H.323 and SIP Phones on the same 54

O

Online Documentation 17
Options, entering using the Telephone Dialpad . . . 108
Options, for 4600 Series IP Telephone Administration 52

P

Pass-Through and Proxy Logoff, 802.1X 90
Port Utilization, TCP/UDP 38
Proxy Logoff and Pass-Through, 802.1X 90
Push Content 171
Push Priorities 172
Push, More Information on 172

Q

QoS 31, 80
DIFFSERV 82
IEEE 802.1D and 802.1Q 81
RSVP and RTCP 85
UDP Port Selection 83
QoS and VoIP 31
QoS, and 4600 Series IP Telephones 80

R

Registration and Authentication, for H.323 35
Registration and Authentication, for SIP 35
Registration, Unnamed 89
Related Documents. 18
Reliability and Performance 42

Requirements 47
Hardware 47
Software 50
Reset Administrative Option 132
Restart the Telephone 134
RSVP and RTCP 85

S

S8300 Media Server, as TFTP Server 72
Script File Parameter Names and Corresponding Media Server Field Names 73
Scripts and Application Files, for 4600 Series IP Telephones 74
Security 44
Settings File, Contents of 78
SIGnaling Protocol Identifier procedure 77
Signaling, Audio and Management 39
SIP and H.323, administering on same network . . . 54
Site-Specific Option Number, customizing 108
SNMP and VoIP 32
Software Alternatives, for DHCP 58
Software Checklist 56
Software Requirements 50
Supplicant Operation, 802.1X 91
System Parameter Values, Impact of TLVs on 95
System Values, Resetting 135

T

Tandem Coding 29
TCP/UDP Port Utilization 38
Telephony Protocols 29
Terms Used in This Guide 14
TFTP 30, 71
TFTP and VoIP 30
TFTP Generic Setup 72
TFTP Server on S8300 Media Server 72
TFTP Server Setup 71
Thin Client Directories, Administering the 169
Time and Date, Setting on SIP IP Telephones 110
TLVs, Impact on System Parameter Values 95
Troubleshooting
the 4601 IP Telephone 145
Troubleshooting Guidelines 123

U

UDP/TCP Port Utilization 38
Unnamed Registration 89
Upgrade Script and Application File, Choosing the Right 76
Upgrade Script, contents of 78, 173

V

View Administrative Option 135
VLAN Considerations 86
VLAN Detection 87
VLAN Separation 78, 88
VLAN Separation Rules 88
VLAN Separation, Option 176 61
VLAN Tagging 86
Voice over IP. See VoIP 27
VoIP 27
Delay and Jitter 28
DHCP 29
H.323 Standard 29
IP Address Lists and Station Number Portability . . 43
NAT 31
Network Assessment 32
Overview, Voice over IP and Network Protocols . . 27
QoS 31
Reliability and Performance 42
Security 44
SNMP 32
Tandem Coding 29

W

WAN Considerations, for 4600 Series IP Telephones 35
Web Sites for Other 4600 Series IP Telephones . . 167
Web Sites, Creating for the 4630/4630SW IP Telephone 151
What's New 13